Guide for

Integrated Software Quality Management (ISQM)

September 2012

GUIDE FOR

INTEGRATED SOFTWARE QUALITY MANAGEMENT (ISQM)
SEPTEMBER 2012

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

ABS Plaza
1701 City Plaza Drive
Spring, TX 77389 USA

Foreword

The marine and offshore industries are increasingly relying on computer-based control systems; therefore the verification of the software used in control systems and their integration into the system is an important element within the overall safety assessment. Accordingly, ABS is introducing this *Guide for Integrated Software Quality Management (ISQM)*. Compliance with the procedures and criteria given in this Guide may result in the granting of the optional notation **ISQM** to a vessel or offshore unit.

ISQM is a risk-based software development and maintenance process built on internationally recognized standards. The ISQM process verifies the software installation on the facility and then monitors for consistency when there are software updates or a change in hardware. ISQM provides a process to manage software over the vessel's or offshore facility's life. The benefit to the Owner and Driller or Crew Organization is an increased level of confidence in software reliability with the goal of increasing safety, decreasing commissioning time, decreasing downtime, and reducing the risk of software related incidents.

As control systems for marine and offshore vessels or units become increasingly more complex and highly integrated, successful implementation relies heavily on the software developed by multiple vendors and the interfaces required for the integration of the software. The ABS *ISQM Guide* places emphasis on the verification of the integration of multiple software packages.

This Guide is meant to be used with other Rules and Guides issued by ABS and other recognized Industry Standards.

This Guide becomes effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of this Guide is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

GUIDE FOR

INTEGRATED SOFTWARE QUALITY MANAGEMENT (ISQM)

CONTENTS

SECTION 1 General....13

1 Scope and Application *(1 September 2012)*....13

3 Basis of Notation *(1 September 2012)*....13

3.1 Extent of Notation....14

5 Documentation....14

5.1 Required Plans and Documentation to Be Submitted (1 September 2012)....14

7 References....14

9 Abbreviations, Acronyms and Definitions....16

SECTION 2 Introduction....17

1 Background....17

1.1 Software Development Life Cycle (SDLC) (1 September 2012)....17

1.3 Support Processes....18

3 Stakeholder Roles and Responsibilities....18

3.1 Roles of Organizations (1 September 2012)....19

5 Use of Terms....21

5.1 Explanation of Software Module....22

5.3 Verification....23

7 ISQM Process....26

7.1 Project Management (PM) and Software Development Life Cycle (SDLC)....27

7.3 Concept Phase (C) (1 September 2012)....27

7.5 Requirements and Design Phase (RD) (1 September 2012)....28

7.7 Design Group and Production Software (1 September 2012)....28

7.9 Construction Phase (CON) (1 September 2012)....30

7.11 Verification, Validation and Transition (V V&T) Phase (1 September 2012)....31

7.13 Operation and Maintenance (O & M) Phase (1 September 2012)....31

FIGURE 1 Integrated Best Practices Approach *(1 September 2012)*....18
FIGURE 2 Organization Interaction: Owner, SBI, DCO, SI and Independent Auditor *(1 September 2012)*....19
FIGURE 3 Organization Interaction: System Integrator, Suppliers or Subcontractors and Independent Auditor *(1 September 2012)*....21
FIGURE 4 Example Relationship of Components, Functions and Software Module....22
FIGURE 5 Closed Loop Verification Example....24
FIGURE 6 Software-In-the-Loop Verification....25
FIGURE 7 Hardware-In-the-loop Verification....26
FIGURE 8 Integrated Software Quality Management Stage Gate Approach *(1 September 2012)*....26
FIGURE 9 SDLC Design Group or Concept and RD Phase Decision Tree *(1 September 2012)*....30
FIGURE 10 Software Flow and Reporting Flow during the V V&T Phase *(1 September 2012)*....31

SECTION 3 Software Development Life Cycle: Concept Phase....33

1 Scope....33
1.1 Concept Phase Activities (1 September 2012)....34
1.3 Concept Phase Organizations Activities....36
3 Example Concept Phase Process Flow for ISQM....36
3.1 Scope and Magnitude (1 September 2012)....36
3.3 Identify Functionality of Functions....36
3.5 Integrity Level Assignment....36
3.7 Write Concept of Operations Documents (ConOps)....36
5 Risk Management *(1 September 2012)*....36
5.1 Safety Reviews and New Technology....37
5.3 Integrity Level (IL) assessment....37
5.5 IL Assignment Functions Documentation Requirements....39
5.7 Software Quality Management....42
5.9 Obsolescence Plans....43
7 Concept of Operations Document (ConOps) *(1 September 2012)*....43
7.1 General Topics....43
7.3 Definition of the Project Scope....44
7.5 Integrated System Major Components and boundary....44
7.7 Constraints....44
9 Deliverables....45
11 Milestones *(1 September 2012)*....45

11.1 Concept Phase Complete, Milestone M2 45
11.3 Authorization from the Owner to Proceed to the RD Phase 46

TABLE 1 Integrity Level Table *(1 September 2012)* 39
TABLE 2 Recommended Safety and Environmental Overall Control System IL Assignments *(1 September 2012)* 41

FIGURE 1 General Flow of Work During the Concept Phase *(1 September 2012)* 36

SECTION 4 Software Development Life Cycle: Requirements and Design (RD) Phase 47

1 Scope and Objectives 47
1.1 General 48
1.3 RD Phase Activities 48
3 Example RD Phase Design Process Flow for ISQM 50
3.1 Criteria and Standards Selection (1 September 2012) 50
3.3 Models 50
3.5 Identify Coding Units and Test Plans 50
3.7 RD Documents 50
5 Requirements and Design Phase Documents 50
5.1 Software Requirements Specification (SRS) 51
5.3 Software Design Specification (SDS) (1 September 2012) 51
5.5 Risk Management 51
5.7 Document Approval (1 September 2012) 52
5.9 Function Requirements for ConOps with IL assignment 52
7 V & V activities during the RD Phase 53
9 RD Phase Deliverables 53
11 RD Phase Complete, Milestone M3 53

FIGURE 1 General Flow of Work During the Requirements and Design Phase *(1 September 2012)* 50

SECTION 5 Software Development Life Cycle: Construction Phase 54

1 Scope and Objectives *(1 September 2012)* 54
1.1 Construction Phase Activities 55
3 Example Construction Phase Process Flow for ISQM 56
3.1 Requirements Translated and Coded 57
3.3 Components Tested 57
3.5 Integration Plans 57
3.7 Creating Construction Document (1 September 2012) 57

5 Construction Phase Document....57
5.1 General Topics....57
5.3 Risk Management....57
5.5 Document Approval (1 September 2012)....58
7 V & V Activities during the Construction Phase....58
7.1 V & V Reviews (1 September 2012)....58
9 Construction Phase Deliverables *(1 September 2012)*....58
11 Construction Phase Complete, Milestone M4 *(1 September 2012)*....58

FIGURE 1 General Flow of Work During the Construction Phase *(1 September 2012)*....56

SECTION 6 Software Development Life Cycle: Verification, Validation and Transition Phase....59

1 Scope *(1 September 2012)*....59
1.1 Review of V&V Report....60
1.3 Scan for Viruses and other Malicious Software Prior to Verification Activities....60
1.5 V&V Review of the Simulation....61
3 Objective *(1 September 2012)*....61
5 V V&T Methods *(1 September 2012)*....61
5.1 Closed Loop Verification....61
5.3 Software-In-The-Loop Verification....62
5.5 Hardware-In-The-Loop Verification....62
7 Defect Ranking....62
7.1 Integrity Level and Defect Category....63
9 V&V Plan *(1 September 2012)*....64
9.1 V&V Plan Description....64
9.3 V&V Plan Approval....69
11 Verification and Validation Report (V&V Report) *(1 September 2012)*....69
11.1 V&V Report Reviews....70
13 System Integrator's Operation and Maintenance (O & M) Plan and Operating Manual *(1 September 2012)*....70
15 V V&T Phase, Verification Accepted, Milestone M5 *(1 September 2012)*....70
17 Deliverables *(1 September 2012)*....70
19 V V&T Phase, Validation and Acceptance, Milestone M6 *(1 September 2012)*....70
21 Transition *(1 September 2012)*....70
21.1 Operations and Maintenance Plan (O&M Plan)....71

TABLE 1 Defect Categories *(1 September 2012)*....62

TABLE 2 IL Ranking and Defect Category, Requirements and Recommendations *(1 September 2012)*Owner may Require Defect Correction....63

FIGURE 1 Software and Reporting Flow during the V V & T Phase *(1 September 2012)*....60
FIGURE 2 IL0 Verification Process Diagram....65
FIGURE 3 IL1 Verification Process Diagram....66
FIGURE 4 IL2 Verification Process Diagram *(1 September 2012)*....67
FIGURE 5 IL3 Verification Process Diagram *(1 September 2012)*....68
FIGURE 6 V&V Organizations Independence from SI Organization by IL Assignment *(1 September 2012)*....69

SECTION 7 Software Development Life Cycle: Operation and Maintenance Phase....72

1 Scope *(1 September 2012)*....72
1.1 Scan for Viruses and other Malicious Software....72
3 Review of the O&M Artifacts *(1 September 2012)*....72
3.1 Operation & Maintenance Plan (O & M Plan)....73
3.3 Owner's Management of Change (MOC) Policy....74
3.5 Software Registry....74
3.7 Control Equipment Registry....75
3.9 Software Change Control Process....76
3.11 Software Configuration Management Plan....76
5 Integrated Control System Maintenance....76
5.1 Scheduled Upgrades – New Functionality....76
5.3 Unscheduled Upgrades (1 September 2012)....78
7 System Retirement....78
9 O & M Phase, Milestone M7....78

TABLE 1 O & M Phase Artifacts *(1 September 2012)*....72

FIGURE 1 ISQM SDLC Phase *(1 September 2012)*....77

SECTION 8 Surveys After Construction and Maintenance of Class....79

1 General....79
3 Surveys for the Integrated Software Quality Management Notation....79
3.1 Survey Intervals and Maintenance Manuals/Records....79
3.3 Annual Surveys....79
3.5 Special Periodical Surveys....80
5 Modifications, Damage and Repairs....80

SECTION 9 Software Development Life Cycle: Design Group *(1 September 2012)*..... 81

1 Scope and Objectives.....81

1.1 General.....81

1.3 Requirements for Use of Functional Description Documents.....82

1.5 Design Group Activities..... 82

3 Example Design Phase Process Flow for ISQM..... 82

3.1 Scope and Magnitude.....83

3.3 Identify Existing Functions and New Functions..... 83

3.5 Owner Assigns the Integrity Level..... 83

3.7 Develop Models.....84

3.9 Safety Reviews and Failure Mode, Effect and Criticality Analysis.....84

3.11 Identify Coding Units and Test Plans..... 84

3.13 Proceed to Construction Phase..... 84

5 Risk Management.....84

5.1 Integrity Level..... 84

5.3 Safety Reviews and FMECA..... 84

5.5 New or Unproven Technology.....84

7 Functional Description Document (FDD).....85

7.1 Requirements of the ISQM System Integrator's FDD.....85

7.3 Requirements of the ISQM SI's Control System Supplier's Section of the FDD.....86

9 V & V activities during the Design Group.....87

11 Deliverables.....87

13 Milestones.....87

13.1 Design Group Complete, Milestone M3.....87

13.3 Authorization from the Owner to Proceed to the Construction Phase..... 87

FIGURE 1 General Flow of Work During the Design Group *(1 September 2012)*..... 83

APPENDIX 1 Activities and Requirements of Organizations *(1 September 2012)*.....88

1 Concept Phase Activities.....89

1.1 Concept Phase Owner's (OW) Activities..... 89

1.3 Concept Phase Driller or Crew's (DCO) Activities..... 91

1.5 Concept Phase System Integrator's (SI) Activities..... 91

1.7 Concept Phase Subcontractors'(CT) Activities.....93

1.9 Concept Phase Verification & Validation (V & V) Activities.....93

1.11 Concept Phase Independent Auditor's (IA) Activities..... 94

3 Requirements and Design (RD) Phase Activities..... 94

3.1 RD Phase Owner's (OW) Activities..... 94
3.3 RD Phase Driller or Crew's (DCO) Activities..... 95
3.5 RD Phase System Integrator's (SI) Activities..... 95
3.7 RD Phase Subcontractors'(CT) Activities..... 96
3.9 RD Phase Verification & Validation (V&V) Activities..... 96
3.11 RD Phase Independent Auditor's (IA) Activities..... 97
5 Construction (CON) Phase Activities.....97
5.1 Construction Phase Owner's (OW) Activities..... 97
5.3 Construction Phase Driller or Crew's (DCO) Activities.... 98
5.5 Construction Phase System Integrator's (SI) Activities... 98
5.7 Construction Phase Subcontractors'(CT) Activities..... 99
5.9 Construction Phase Verification & Validation (V&V) Activities.....99
5.11 Construction Phase Independent Auditor's (IA) Activities.....100
7 Verification, Validation and Transition (V V&T) Phase Activities. 101
7.1 Verification & Validation Phase Owner's (OW) Activities.....101
7.3 Verification & Validation Phase Driller or Crew's (DCO) Activities..... 101
7.5 Verification & Validation Phase System Integrator's (SI) Activities.....102
7.7 Verification & Validation Phase Subcontractors'(CT) Activities.....102
7.9 Verification & Validation Phase Verification & Validation (V&V) Activities..... 103
7.11 Verification & Validation Phase Independent Auditor's (IA) Activities.....104
9 Operation and Maintenance (O & M) Phase Activities..... 105
9.1 Operation and Maintenance Phase Owner's (OW) Activities.....105
9.3 Operation and Maintenance Phase Driller or Crew's (DCO) Activities..... 105
9.5 Operation and Maintenance Phase System Integrator's (SI) Activities.....106
9.7 Operation and Maintenance Phase Subcontractors' (CT) Activities..... 106
9.9 Operation and Maintenance Phase Verification & Validation (V & V) Activities..... 106
9.11 Operation and Maintenance Phase Independent Auditor's (IA) Activities.....106

APPENDIX 2 Definitions and Abbreviations.....107
1 Definitions *(1 September 2012)*.....107
3 Abbreviations *(1 September 2012)*..... 112

APPENDIX 3 Concept Phase 115

1 Example Concept of Operations Document *(1 September 2012)* 115

3 Example Obsolescence Management Plan Outline 118

5 ConOps Traceability *(1 September 2012)* 119

5.1 Example of Traceability Matrix 120

APPENDIX 4 Requirements and Design Phase 122

1 Software Requirements Specification 122

1.1 Example of Software Requirements Specification Table of Contents 122

3 Software Design Specification 123

3.1 Example of Software Design Specification Table of Contents 123

5 Models 125

5.1 Models 125

FIGURE 1 126

FIGURE 2 127

FIGURE 3 128

FIGURE 4 129

FIGURE 5 130

FIGURE 6 131

FIGURE 7 132

APPENDIX 5 Construction Phase 133

1 Software Coding and Testing 133

1.1 Software Integration (1 September 2012) 134

1.3 Software SI Integration Testing 134

3 Management 134

3.1 Organization 135

3.3 Software Configuration Management Responsibilities 135

3.5 Software Configuration Management Plan Implementation 135

3.7 Applicable Policies, Directives, and Procedures 135

5 SCM Activities 136

5.1 Configuration Identification 136

5.3 Change Control 137

5.5 Configuration Status Accounting 137

5.7 Audits and Reviews 138

7 Tools, Techniques, and Methodologies 138

9 Supplier Control 138

11 Records Collection and Retention 138

APPENDIX 6 Verification, Validation and Transition Phase..... 140
1 Example V&V Plan Outline *(1 September 2012)*..... 140
3 Grouping of Software Modules..... 142

APPENDIX 7 Operation and Maintenance Phase..... 143
1 Recommended ISQM Maintenance Personnel's Activities 143
3 Example O & M Plan Table of Contents..... 144
3.1 Example of Maintenance Plan..... 144
3.3 Example of Operation and Maintenance Plan Outline (1 September 2012)..... 145
3.5 Control System Hardware, Firmware and Software Retirement Plan..... 147
5 Software Change Control Process *(1 September 2012)*..... 148
7 Example Software Control Form Process Flow..... 150
9 Example MOC Process..... 152
11 Obsolete Control System Components Considerations..... 154

FIGURE 1 Recommended Management of Change Process..... 152

APPENDIX 8 Project Management..... 155
1 Scope..... 155
3 Background..... 155
5 PM Process Groups..... 157
5.1 PM Initiating Group..... 157
5.3 PM Planning Group..... 158
5.5 PM Executing Group..... 159
5.7 PM Monitoring and Control Group..... 160
5.9 PM Closing Group..... 161
7 Software Project Management Plan (SPMP)..... 161
8 **Table of Contents** 162
9 Introduction..... 162
9.1 Project Overview..... 162
9.3 Project Deliverables..... 162
9.5 Evolution of the SPMP..... 162
9.7 Reference Materials..... 162
9.9 Definitions and Acronyms..... 163
11 Project Organization..... 163
11.1 Process Model..... 163
11.3 Organizational Structure..... 163
11.5 Organizational Interfaces..... 163
11.7 Project Responsibilities..... 164
13 Managerial Process..... 164
13.1 Management Objectives and Priorities..... 164
13.3 Assumptions, Dependencies, and Constraints..... 164

13.5 Risk Management....164
13.7 Monitoring and Controlling Mechanisms....165
13.9 Staffing Approach....165
15 Technical Process....165
15.1 Methods, Tools, and Techniques....165
15.3 Software Documentation....165
15.5 User Documentation....166
15.7 Project Support Functions....166
17 Work Packages, Schedule, and Budget....166
17.1 Work Packages....166
17.3 Dependencies....166
17.5 Resource Requirements....166
17.7 Budget and Resource Allocation....166
17.9 Schedule....166
19 Additional Components....167
19.1 Index....167
19.3 Appendices....167
21 Software Quality Assurance Discussion....167
21.1 Software Process and Product Metrics....167
23 Metrics *(1 September 2012)*....168

TABLE 1 39 Project Processes....156

FIGURE 1 Project Management Process Groups Relationship to SDLC....157

APPENDIX 9 Design Group *(1 September 2012)*....169
1 Activities and Submittals for Design Group....170

SECTION 1
General

1 Scope and Application *(1 September 2012)*

This Guide presents the procedures and criteria to be employed by ABS in the review and survey of computer based control systems involving software development. The objective of the Guide is to reduce software related incidents that could negatively affect the performance of such systems. Compliance with the procedures and criteria given in this Guide may result in the granting of the optional notation **ISQM** to a vessel or offshore unit.

This Guide emphasizes the software aspect of control systems. Criteria for the hardware, Failure Mode and Effect Analysis (FMEA), and security of computer based control systems are given in other Rules, Guides and other standards issued by ABS. These other criteria are to be satisfied in addition to those given in this Guide.

The procedures and criteria given in this Guide rely on a structured process, based on best practices, for the engineering management of the software development process in the design, construction and maintenance of computer based systems. Compliance with the process and criteria of this Guide is intended to increase safety, accessibility, reliability, and ease of maintenance of computer based control systems.

This Guide is applicable to stand-alone or integrated computer based control systems. Such a computer based control system can be installed on a ship, offshore unit, fixed and floating offshore installation, or other type of facility. The computer based system can be associated with a control system of any level of complexity, including those used for propulsion and navigation.

The procedures and criteria given in this Guide will involve a variety of parties concerned with software development and maintenance. These include Systems Integrators (SI), Driller or Crew Organization (DCO), Ship Builder Integrator (SBI) or the Shipyard, Verification and Validation Organizations (V&V), Independent Auditor (IA), Owner, Suppliers, and Subcontractors involved in integrated system software development, implementation, operation and maintenance. It is the Ship Builder Integrator (Shipyard) and/or Owner's (refer to 2/3.1.1) responsibility to verify that the other involved parties are aware of the need to comply with this Guide.

3 Basis of Notation *(1 September 2012)*

The **ISQM** notation indicates compliance with the procedures and criteria given in this Guide for software development from the *concept* phase or *Design Group* to the end of the *Verification, Validation and Transition* phase (Refer to Sections 2 to 6, and Section 9 for *Design Group*, herein); subsequently, leading to the beginning of operation of the affected system. Maintenance of the **ISQM** notation over the operational life of the system is subject to the periodic surveys carried out on board the vessel or unit in accordance with Section 8 of this Guide.

Integrated or non-integrated control systems affected by and classed with the **ISQM** (for integrated control system) and **SQM** (for non-integrated control system) notation will be listed in the ABS *Record* to describe the exact coverage of the notation. For example, the describer could be one or more of the following:

- Dynamic Positioning Control System
- Drilling Control System
- Vessel Management Control System
- Hydraulic Power Unit's Control System
- Power Management Control System
- etc.

3.1 Extent of Notation

When the **ISQM** notation is given to a control system, the connected control systems of the controlled equipment and functions are not included in the notation. However, the interface between the ISQM control system and other connected control systems are included in the Guide.

The term "approved" or "approval" is to be interpreted to mean that the plans, reports or documents have been or are to be reviewed for compliance with one or more of the Rules, Guides, standards or other criteria of ABS.

5 Documentation

5.1 Required Plans and Documentation to Be Submitted *(1 September 2012)*

In order to receive the **ISQM** notation, plans and documentation, as applicable, are to be submitted by the responsible organization.

For plans and data to be submitted for approval, refer to Appendix 1 of this Guide.

7 References

IEEE Std 14764-2006, Second edition 2006-09-01, *Software Engineering – Software Life Cycle Processes – Maintenance*

IEEE Std 12207-2008 Second edition, 2008-02-01, *Systems and Software Engineering – Software Life Cycle Processes*

IEEE Std 730™-2002 *IEEE Standard for Software Quality Assurance Plans*

IEEE Std 828™-2005, *IEEE Standard for Software Configuration Management Plans*

IEEE Std 829™-2008, *IEEE Standard for Software and System Test Documentation*

IEEE Std 830-1998, *IEEE Recommended Practice for Software Requirements Specifications*

IEEE Std 1012™-2004, *IEEE Standard for Software Verification and Validation*

IEEE Std 1016-1998, *IEEE Recommended Practice for Software Design Descriptions*

IEEE Std 1219-1998, *IEEE Standard for Software Maintenance*

IEEE Std 1362™-1998 (R2007), *IEEE Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document*

IEEE Std 1490™-2003, *IEEE Guide Adoption of PMI Standard A Guide to the Project Management Body of Knowledge*

IEEE SWEBOK 2004, *Software Engineering Body of Knowledge*

IEC 61508-0 (2005-01), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

IEC 61508-1 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC 61511-1 (2003-01), *Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 61511-2 (2003-07), *Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1*

IEC 61511-3 (2003-03), *Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

ISO/IEC 9126-1:2001 *Software engineering – Product quality – Part 1: Quality model*

ISO 17894-2005 *General principles for the development and use of programmable electronic systems in marine applications*

ISO 9001:2008 *Quality Management Systems – Requirements*

ANSI/ISA-84.00.01-2004 Part 2 (IEC 61511-2 Mod) *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative*

Department of Defense and US Army: *Practicable Software & System Measurement A Foundation for Objective Project Management*

9 Abbreviations, Acronyms and Definitions

For abbreviations, acronyms, and definitions used throughout this Guide, refer to Appendix 2.

SECTION 2
Introduction

1 Background

This Guide prescribes the best practices for the engineering management of the software development process for the design, construction and maintenance of integrated computer-based control systems. This section presents an overview of the phases and management practices with a goal of successful development and deployment of the software. There are five Software Development Life Cycle (SDLC) phases, one overall project management and eight milestones or stage gates. The SDLC depicted in this Guide is the minimum acceptable process. Milestone requirements are to be met before leaving a phase. The milestones verify that open issues are being addressed in a systematic manner and the documentation from the functions are detailed sufficiently to convey meaning and intent. There are three topics of significance in the successful development and deployment of software, with some overlap. These topics are:

i) The Software Development Life Cycle (SDLC)

ii) Project Management Practices (refer to Appendix 8)

iii) Support Processes

This Guide is focused on the SDLC.

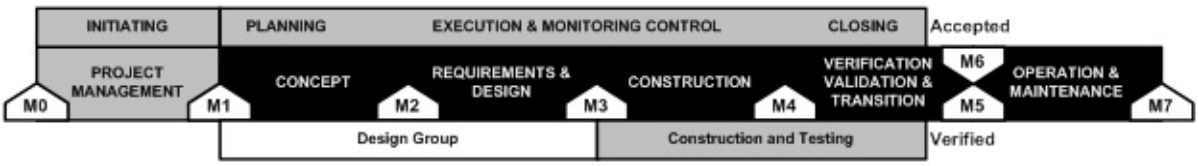
1.1 Software Development Life Cycle (SDLC) *(1 September 2012)*

The SDLC is the engineering plan for software development from concept to retirement of the computer-based control system.

This Guide follows industry standard practices, IEEE Std 12207-2008 Second edition, 2008-02-01, *Systems and software engineering — Software Life Cycle Processes* which is the basis of the SDLC denoted in black in 2/1.1 FIGURE 1. The Design Group allows for the use of "Production Software" (Section 9) where the System Integrator provides Functional Description Documents to replace the documents from the Concept and Requirements & Design Phases. The project management phases of IEEE Std 1490™-2003, *IEEE Guide Adoption of PMI Standard*, *A Guide to the Project Management Body of Knowledge* are denoted in grey. The SDLC below depicts five phases. Milestones (or stage gates) are often associated with distinct points within or at the boundaries of phases of an SDLC and are tied to the delivery of specific stage products.

A more detailed discussion of each phase of the SDLC is found in the individual phase Sections 3 through 7 and Section 9. Project Management is discussed in Appendix 8.

FIGURE 1
Integrated Best Practices Approach *(1 September 2012)*



1.3 Support Processes

Support processes provide tools for the design, construction and maintenance of integrated control systems. These processes are implemented within the early stages of the SDLC and specific deliverables are defined. Support processes are especially critical to the Operations and Maintenance Phase of the lifecycle where a large portion of the re-configuration, new functionality and update effort is expended. The following support processes are necessary:

i) Training

ii) Management of Change

iii) Configuration Management of hardware and software

iv) Acceptance testing of all system changes

v) Independent audit of change management

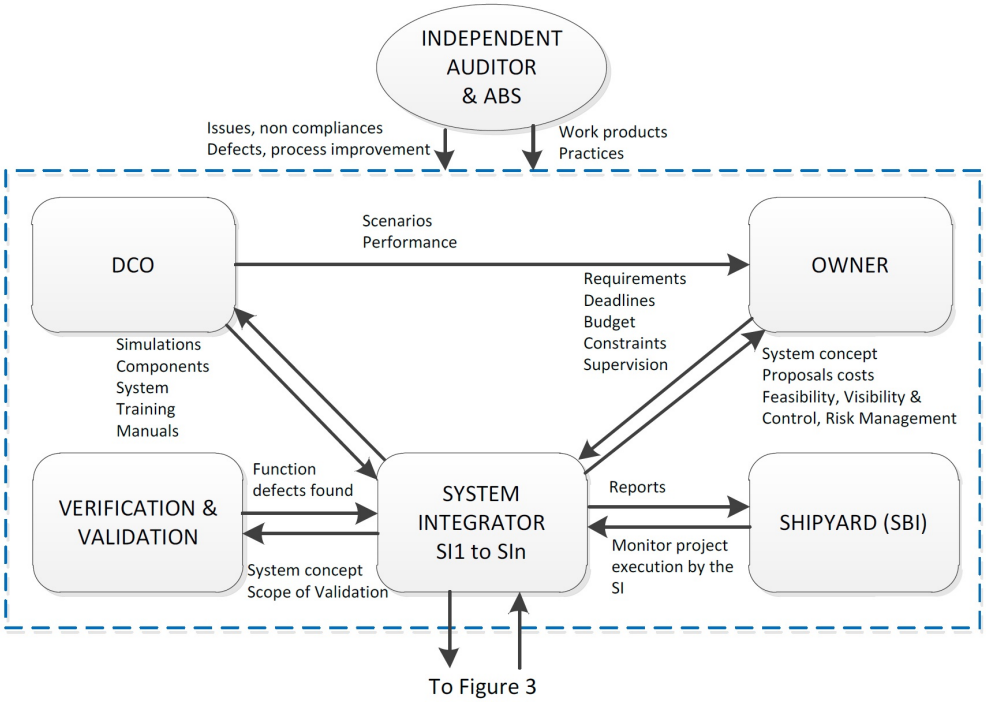
vi) Metrics

3 Stakeholder Roles and Responsibilities

There are numerous roles required for the development and deployment of software systems. Terminology of a SDLC may vary from organization to organization, however the intent is the same. The SDLC process contains requirements, activities and deliverables. The SDLC requirements and activities are to be executed by various organizations. The requirements and activities for the organizations are listed in Appendix 1.

The organization interaction, flow of information and the timeliness of the information are factors in maintaining the project's schedule. Section 2, Figure 2 shows typical information flow between key stakeholder organizations.

FIGURE 2
Organization Interaction: Owner, SBI, DCO, SI and Independent Auditor *(1 September 2012)*



3.1 Roles of Organizations *(1 September 2012)*

The stakeholder organizations are defined below. In some cases, the organization's responsibilities may be combined (i.e., The Owner could also be the DCO and/or IA; The Owner could be the SBI (Builder or shipyard) during initial construction; System Integrator (SI) could also be the Verification and Validation (V&V) organization). This Guide assumes the responsibilities and activities are performed by the organization assigned those activities. The activity assignments clarify the roles and deliverable per organization per phase.

3.1.1 Owner Organization (OW)

The Owner is the organization who provides funding and initiates the project. The SBI is accountable (per contract) for the delivery of the contracted ISQM control system(s), as selected by the Owner, on the asset.

3.1.2 System Integrator Organization (SI)

The System Integrator is responsible for the development of the integrated system. Depending upon the selection of ISQM systems, there may be several System Integrator Organizations. The System Integrators are the experts of their respective control system and have integration awareness of connected equipment's control system requirements. The SI is responsible for the design of the integrated system, creation of the SRS & SDS (Section 4) or the FDD (Section 9), supplier management, integration and with the Owner's permission, verification of the control system software. The Owner may request input from the SI, as needed, for the development of the ConOps. The Owner may select the SI to perform the verification of the integrated system or the Owner may select an independent third party. The SI or SBI organizations are not to transfer responsibilities when delegating SI activities to a third party. If the project size does not warrant a SI, then these responsibilities are to be taken by Owner, DCO or a Supplier organization as selected by the Owner.

i) SI organization is to have a current ISO 9001 or be CMMI level 2 maturity level qualified or higher.

ii) Other software quality management systems may be specially considered by ABS. Please contact ABS.

It is recommended that the System Integrator and the Shipyard make Suppliers aware of the verification requirements and activities.

3.1.3 Driller or Crew Organization (DCO)

The Driller or Crew (DCO) is the user of the integrated system and could also be the Duty Holder, drilling contractor or lessee. The DCO is responsible for the Operation and Maintenance Phase of the system. Maintenance responsibility facilitates continued reliable operation of the integrated system as improvements, upgrades and replacements or new components are added to the system over its lifetime.

3.1.4 Verification & Validation Organization (V&V)

The V & V organization is to verify the software as defined in the Software Requirement Specification (SRS) and integrated Software Design Specification (SDS) using Closed Loop (specially considered), Software-In-the-Loop, Hardware-In-the-Loop or a combination of the three methods. The V & V organization may be part of the System Integrator's organization or may be independent, as directed by the Owner, with limitation. Refer to 6/9.1 FIGURE 6.

3.1.5 Independent Auditor Organization (IA)

The IA organization monitors involved parties, including Suppliers for compliance with this Guide, produces reports for the Owner and/or SBI, DCO & System Integrator. The IA Organization is to be independent from the SI's software development team(s). The IA team is to coordinate with ABS, the Owner and the SBI on IA activities. The IA team may assist the Owner with validation of the system. During the Verification, Validation and Transition Phase (V V&T), the Concept Phase documents are reviewed by the Owner, DCO and IA Organizations to facilitate subsequent validation to the Owner's requirements. The Owner validates (accepts) the integrated control system.

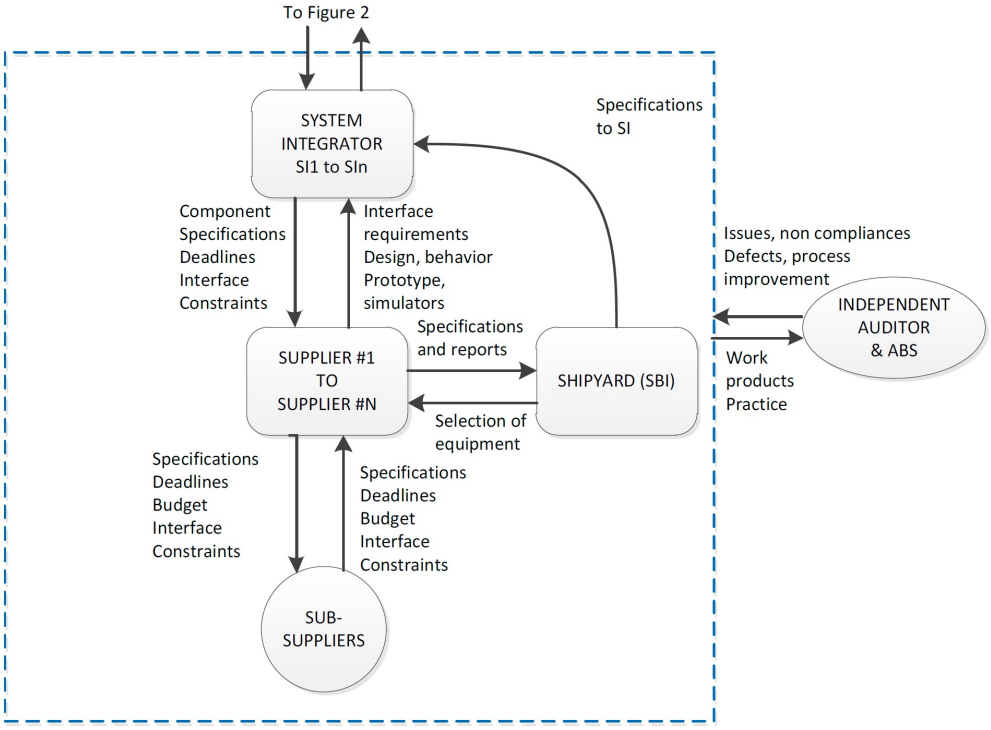
3.1.6 Ship Builder Integrator or Shipyard Organization (SBI)

The Ship Builder Integrator is the shipyard builder. The SBI is to contract with a System Integrator Organization or may use a division within the Shipyard Organization if the division meets the requirements listed for the SI Organization, refer to 2/3.1.2. The SBI has integration verification activities once the ISQM control system(s) is installed. The integration activities include verifying the communication (integration verification) between equipment connected to the ISQM control system(s). The SBI is accountable (per contract) for the delivery of the contracted ISQM control system(s), as selected by the Owner, on the asset.

3.1.7 ABS

ABS reviews documents during the development of the ISQM control system(s). ABS is to witness verification testing of control systems assigned a rating of IL2 or IL3. Refer to 6/9.1 FIGURE 6. ABS is to witness the integration verification performed by the SBI for new builds or the Owner.

FIGURE 3
Organization Interaction: System Integrator, Suppliers or Subcontractors and Independent Auditor *(1 September 2012)*



3.1.8 Supplier or Subcontractor Organization (CT)

The Supplier is any contracted or subcontracted provider of integrated system components or software under the coordination of the System Integrator or Shipyard. The Supplier is to provide specifications and constraints of the control system's package(s) being supplied. The suppliers' verification is to be witnessed by ABS for IL2 and IL3 supplied equipment.

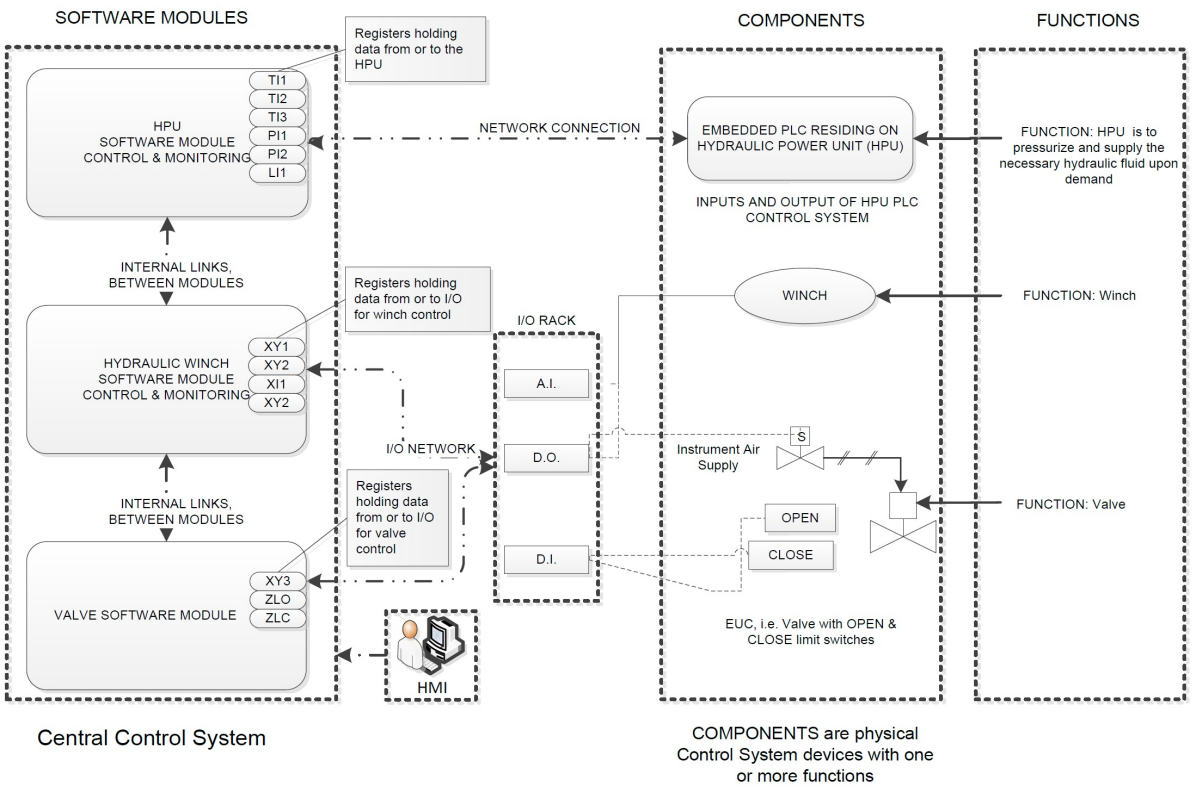
i) CT organization is to have a current ISO 9001 or be CMMI level 2 maturity level qualified or higher.

ii) Other software quality management systems may be specially considered by ABS. Please contact ABS.

5 Use of Terms

Throughout this Guide terms are used with specific meaning. The relationships among function, Software Module and component are shown in 2/5 FIGURE 4.

FIGURE 4
Example Relationship of Components, Functions and Software Module



AI = Analog Input, DO = Discrete (Binary) Output, DI = Discrete (Binary) Input

5.1 Explanation of Software Module

5.1.1 Software Module

Grouping of software code which may contain other modules (code) to monitor, control and alarm. A valve's Software Module may contain:

i) *"Alarm" Software Module:* This software module monitors the time the valve takes to open or close and alarms if the valve did not confirm (through limit switches) that the valve is fully open or closed within the defined time. (If valve equipped with limit switches)

ii) *"Interlock" Software Modules:* Sends a message to other affected functions to either remain in their current position or reverse as the alarm condition (state) of this valve changes.

iii) *"Logic" Software Module:* If there are any interlocks on the opening or closing of the valve, these interlocks are programmed.

iv) *"Diagnostic" Software Module:* The I/O may have diagnostics to monitor the "health" of inputs and outputs for failure.

5.1.2 Component or Package

A physical device, machine or instrument (i.e., HPU unit)

5.1.3 Function

What the Component is to do (e.g., Pressure transmitter has a function of transmitting the pressure signal. The HPU has a function of pressurizing the hydraulic fluid).

5.1.4 Human Machine Interface

Displays the status of the valve and may allow for control of the valve. An example is a graphical user interface.

5.3 Verification

(1 September 2012). There are three verification methods to choose from that are acceptable to ABS.

i) The simulation of the scenarios is to be of sufficient fidelity to verify the integrated system software to the specification. It is permissible to ABS to use a mix of methods to verify the software.

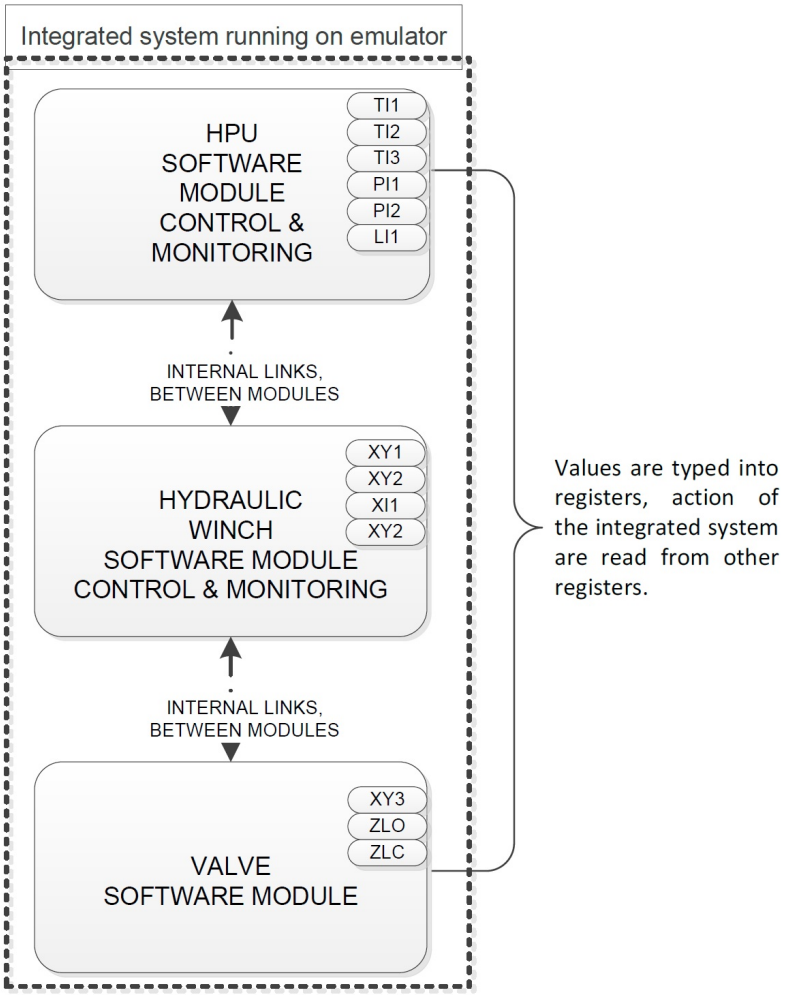
ii) The primary verification method is to be selected by the Owner during the Concept Phase.

iii) It is recommended that the SI state their preferred verification method for consideration by the Owner.

5.3.1 Closed Loop Verification *(1 September 2012)*

Closed Loop verification is acceptable with less complex control systems. In Closed Loop verification, detailed knowledge of the process and programming is necessary to verify correct actions of the software. The register data are interpreted to verify the integrated system's response is per the specifications (SRS and SDS or FDD). The use of Closed Loop Verification will be specially considered by ABS. Refer to 2/5.3.1 FIGURE 5.

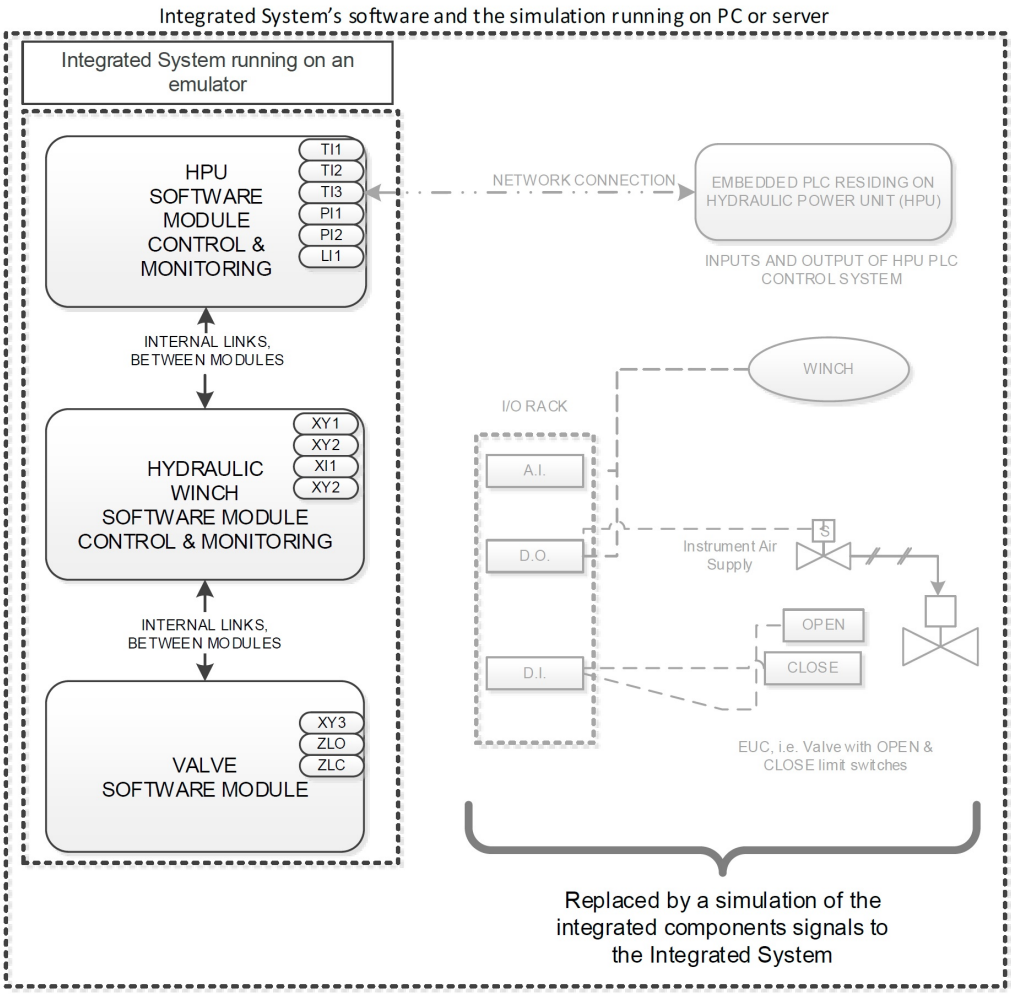
FIGURE 5
Closed Loop Verification Example



5.3.2 Software-In-the-Loop Verification

In Software-In-the-Loop verification, the integrated system program is running (executing) on a non-native computer. Within this computer, a simulation has been programmed to emulate components of the integrated system. The Software-In-the-Loop verification does not verify the networked connections, input or output hardware modules, or the processor. The program is run on an emulator on a PC, server or other computing device. Software-In-the-Loop verification does allow for a number of scenarios to be run to test the integrated system's code. The real world is represented by mathematical models in the simulation program. Refer to 2/5.3.2 FIGURE 6.

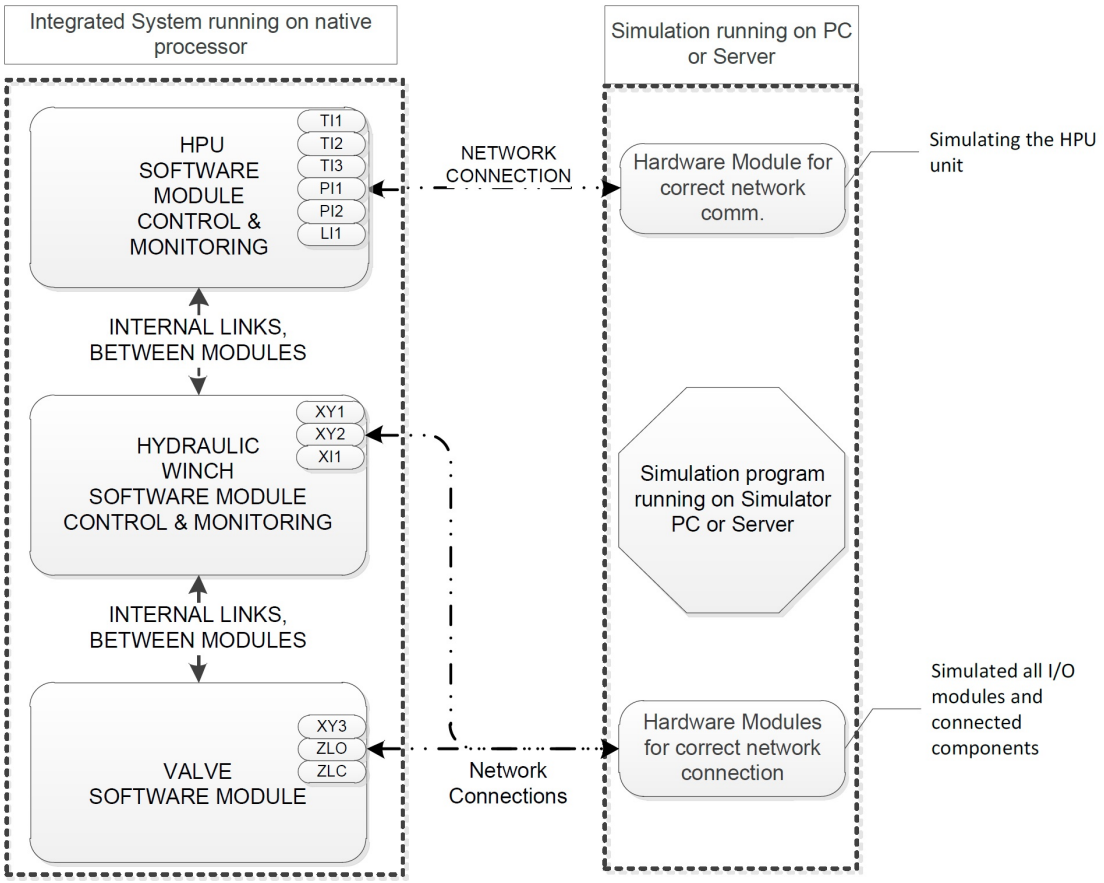
FIGURE 6
Software-In-the-Loop Verification



5.3.3 Hardware-In-the-Loop Verification

The integrated system's program is being executed on its native hardware (native processor, firmware) and the simulation is being executed on a separate machine. Interfaces between the two are developed for the testing. Hardware-In-the-Loop verification does allow for a number of scenarios to be run to test the integrated system's code. The real world is represented by mathematical models in the simulation program. Refer to 2/5.3.3 FIGURE 7.

FIGURE 7
Hardware-In-the-loop Verification

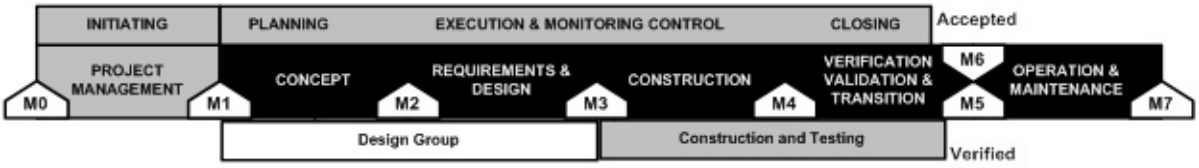


7 ISQM Process

(1 September 2012) Each of the four development phases and the *Design Group* plus the Operation and Maintenance phase are briefly described below. With reference to 2/7 FIGURE 8, individual paragraphs below will describe each of the topics listed in the figure. More detailed descriptions of milestones, deliverables, work flows, and activities are included in Sections 3 through 7 and Section 9 of this Guide. Project Management processes are described in Appendix 8.

Refer to Appendix 1 which contains a listing of activities and requirements for each organization by phase.

FIGURE 8
Integrated Software Quality Management Stage Gate Approach *(1 September 2012)*



7.1 Project Management (PM) and Software Development Life Cycle (SDLC)

7.1.1 Project Management (PM)

Project Management is discussed in Appendix 8. The Project Management (PM) processes are not bound by SDLC phases and milestones, as activities extend beyond SDLC phases. The Project Management Institute has developed a set of project management processes. The basic process groups are:

i) Initiation

ii) Planning

iii) Execution

iv) Monitoring and Controlling

v) Closing

7.1.2 PM Initiating Group

In the Initiating group, the primary objective is the authorization of the project.

7.1.3 PM Planning Group *(1 September 2012)*

In the PM Planning group, the primary purpose is planning the work that needs to be done. It is recommended to include: development of initial schedules, resource plans, scope definition, activity duration estimates, etc. Planning is one of the processes that continue through the life cycle of the project from concept to deployment. There is operation & maintenance planning after the system is deployed.

7.1.4 PM Executing Group

In the PM Executing group, the primary purpose is to get the work done. This includes executing the plan, source selection, contractor management, and team development. The executing group also carries through the lifecycle as activities in each phase are accomplished. The executing group interacts with other PM groups.

7.1.5 PM Monitoring and Control Group

In the Monitoring and Control group, the primary purpose is to measure and assess the work being done. To support variance from the plan, change and schedule control is to be implemented and monitored. Scope management, resource analysis and other indicators that assist in gauging the health of a project are implemented.

7.1.6 PM Closing Group *(1 September 2012)*

In the Closing group, the primary purpose is to close the project. This includes administrative closure, final data gathering and delivery of maintenance manuals, drawing, etc., to the Owner and Driller or Crew (DCO).

7.3 Concept Phase (C) *(1 September 2012)*

The Concept Phase (Section 3) provides the direction and scope of the project. The goal of the Concept Phase is to define the integrated system in sufficient detail to allow for safety review(s), Integrity Level (IL) assessments, and initial integrated system component selection. The IL number is assigned based upon the risk and consequence of a failure of the function. Refer to 3/5.3.4 TABLE 1. Integrated system component identification is first done by determining which functions are allocated to software and which functions are non-computer based system controlled.

After the functions are defined, the Owner is to review consequences of failure of the function and assign an Integrity Level with input from other organizations and groups. Refer to Section 3, Tables 1 and 2.

The Owner is to specify the primary verification method to be followed. There are three options for verification of the integrated system software as mentioned in 2/5.3. In the V V&T Phase, the software for the system is minimally determined to operate as specified in the SRS and SDS or FDD (verification).

It is recommended that the complexity of the functions, the functions' Integrity Level numbers and the quantity of Suppliers' packages that are to be integrated be considered when selecting the primary verification method. The simulation software development is performed in parallel with the integrated system software development and not at the conclusion of the software development.

The main deliverable for this phase is the Concept of Operations document (ConOps). Overall architecture of the system depicting the interoperability of the software is developed. It is recommended that an analysis of the computer-based control system hardware requirements is included so that the system and software requirements are separately identified within the ConOps. The ConOps is used to develop the integrated Software Requirement Specification (SRS) and the integrated Software Design Specification (SDS) in the Requirement and Design Phase. The SRS and SDS are used for verification while ConOps is a portion of the validation process of the computer-based control system. An example of a ConOps is included in Appendix 3. Functions listed in the ConOps are traceable and have been assigned an IL number. The IL number provides for visibility of the important functions and verification scenarios are influenced by the assigned IL number. It may be acceptable for the Owner to request the SI to provide a Functional Design Document (FDD), See 2/7.7 FIGURE 9 and Section 9.

Concept errors in the ConOps may have project schedule implications if the errors are discovered late in the SDLC process.

7.5 Requirements and Design Phase (RD) *(1 September 2012)*

During the Requirements and Design Phase (Section 4), the requirements and detailed specifications of the integrated software functions are developed, modeled, and documented from the ConOps. The goal of the RD Phase is to translate the functions (in light of the system architecture) defined in the ConOps into documents that the System Integrator's developers and programmers can use to construct the software to provide the functions described in the ConOps. Functions are traceable back to the ConOps using some function identifier.

The deliverables from this phase are the integrated Software Requirements Specifications (SRS) and integrated Software Design Specification (SDS), the technical basis of the software developed in the Construction Phase.

The SRS contains the traceable technical details of each function from the ConOps. Verification requirements as specified in the ConOps are added and detailed for the functions.

The SDS contains the traceable design details of each function, communication node and system architecture components being integrated.

Performance, safety, database and security requirements, adherence to standards, ergonomic consideration, and capabilities are to be specified in detail in the RD Phase documents. Integration testing for all commercial off-the-shelf (COTS) packages is to be written as a V & V requirement. The COTS V & V Plan may be developed by the Supplier.

The RD Phase documents details all Owner and/or DCO requirements and the documents are reviewed by the Owner, IA, SBI, and DCO for ConOps compliance. It is recommended that the SRS and SDS clearly indicate to the expected functionality and action of the computer-based control system when there are failures.

7.7 Design Group and Production Software *(1 September 2012)*

The Design Group (Section 9) is the combination of two SDLC phases, Concept and the Requirements & Design Phases.

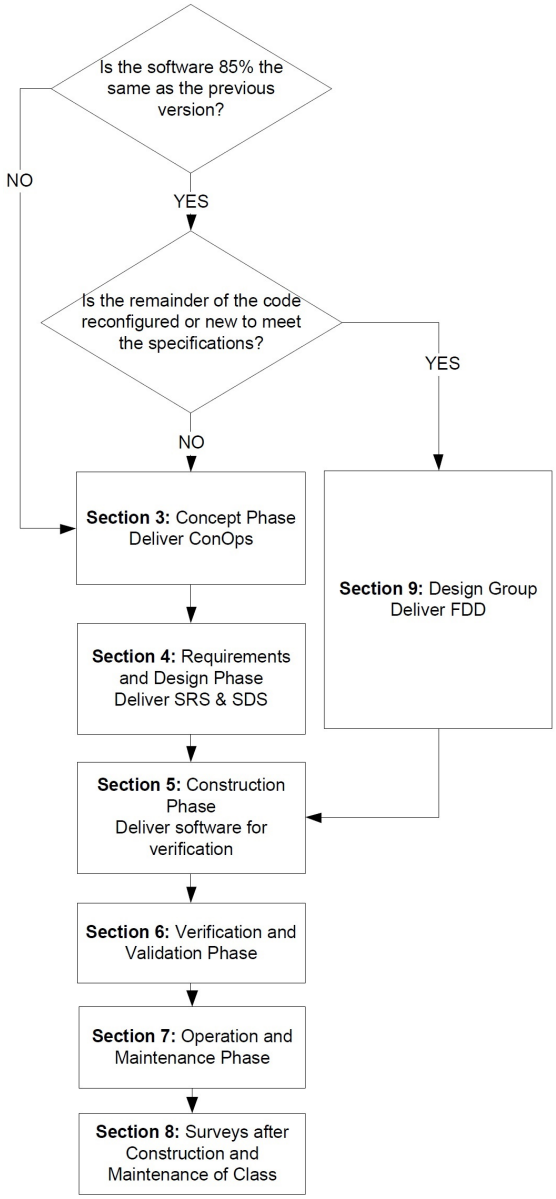
Control systems of equipment may be installed on existing offshore and marine assets, where a relatively small percentage of the code is unique or different from the installed systems, to meet the requirements of the specification. When a majority of the control system software modules or code utilizing established functions and code modules with the remainder being new or modified code to meet the specification.

Since the software is already in use within industry, the submittal documents are reduced. The ConOps and the SRS & SDS are combined into the Functional Description Documents (FDD) and some of the software requirement analysis is reduced. The FDD may be a combination of documents and drawings meeting the requirements from Section 9.

The FDD consists of information and details contained within the ConOps and SRS & SDS. Using the Design Group to develop the FDD does not lessen the verification activities or requirements that occur in the V V&T Phase.

Using the FDD, the Owner, assigns the Integrity Level to the functions. The Owner, SBI, DCO and IA adds normal, degraded or failed control system condition testing scenarios for the verification from their experience or prior knowledge. If the control system functions have been assigned an Integrity Level 2 or 3 (IL2 or IL3), then the System Integrator facilitates and performs a software-focused, top down, functional Failure Mode and Effect Criticality Analysis (FMECA). See 2/7.7 FIGURE 9 for the paths to follow with Design Group or the Concept and RD Phases.

FIGURE 9
SDLC Design Group or Concept and RD Phase Decision Tree *(1 September 2012)*



7.9 Construction Phase (CON) *(1 September 2012)*

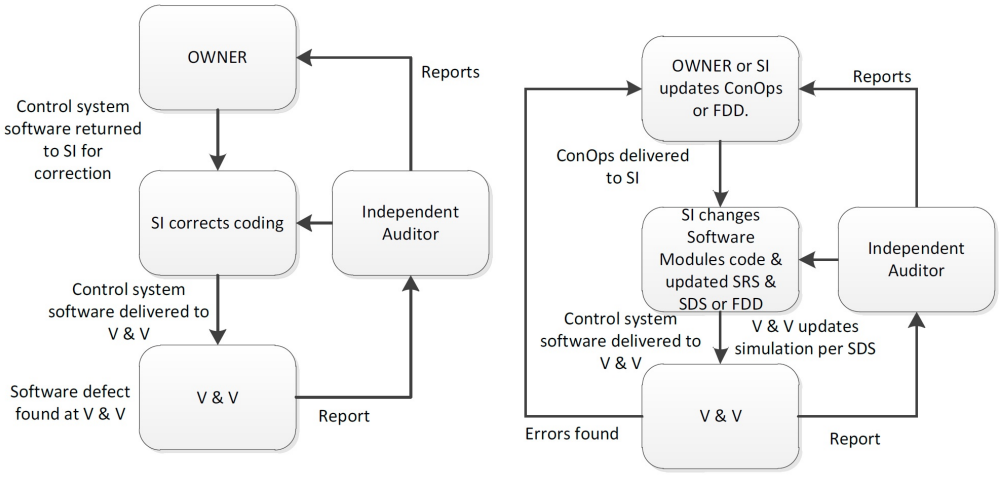
The activities that occur during the Construction Phase (Section 5) are centered on translating the requirements and specifications from the SRS and SDS or FDD into functioning integrated system code. It is recommended that the SI tests the code for compliance with the SRS and SDS or FDD internally. It is also recommended that the SI testing not be limited to basic levels of compiling or individual Software Module testing, extend towards comprehensive internal module and module-to-module testing by the SI.

If any COTS software is part of the system, integration testing is to be performed by the SI to facilitate the verification testing. Testing activities in this phase focus on the software aspects of the system by the SI and suppliers. Verification and demonstration of the software performance and possibly the integration verification occurs in Verification, Validation and Transition Phase. Further integration testing occurs during commissioning of the integrated control systems.

7.11 Verification, Validation and Transition (V V&T) Phase *(1 September 2012)*

In the Concept Phase, the Owner has specified which of the three verification methods is to be used as the primary verification method. In the V V&T Phase (Section 6), the software for the system is determined to operate as specified in the SRS and SDS or FDD. The SRS and SDS or FDD is the governing document(s) for verification. The ConOps or the FDD is a document used for validation as well as for the commissioning and sea trial(s) activities. The V&V organization is to write a plan for verification (V&V Plan) based on the primary method chosen in the Concept Phase and configures the simulator. An example V&V Plan is provided in Appendix 6. The Independent Auditor and ABS are to witness the verification is in accordance with the V&V Plan for selected systems. Any software defects, concept errors or other deficiencies, compared to the SRS, SDS and ConOps or FDD, are to be documented and reported. The SI with input from the V&V, Owner or IA Organizations determines if the deficiency is a control system code defect, simulation code defect or a concept error. Concept errors affect validation and the ConOps and the FDD. The software is returned to the SI group for corrective action.

FIGURE 10
Software Flow and Reporting Flow during the V V&T Phase *(1 September 2012)*



Before the V&V organization can complete verification of the integrated system, the complete V&V Plan is to be performed. The V&V Plan is to verify the integrated software without;

i) Detecting any Critical or Major Defects (Refer to 6/7 TABLE 1 for software defect ranking table)

ii) Detecting any IL2 or IL3 defects or other defects that systemically affect IL2 or IL3 level functions.

Regression testing is used to test the "corrected" software for new defects that may have been introduced during the coding to correct a previously known or detected defect. Regression testing is to include complete testing of all inputs to and outputs from the changed software module that interfaces with any IL2 or IL3 components.

After verification of the completed software, all activities necessary to transition the integrated system to the Owner and DCO are accomplished. The software is installed on the target hardware and support services arranged, as selected by the Owner. The SI submits all documentation to the Owner and DCO.

7.13 Operation and Maintenance (O & M) Phase *(1 September 2012)*

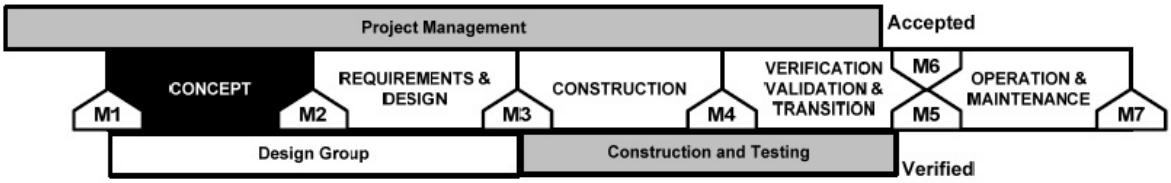
This phase covers the operation and maintenance activities, including scheduled and unscheduled upgrades and problem resolution activities (Section 7). This phase also extends to retirement activities. The responsibilities for activities in this phase lie with the DCO with activities by Suppliers. The SI is to

provide the Operation and Maintenance Plan towards the end of verification activities. Refer to Appendix 7 for an example Operation and Maintenance Plan template.

Most software requires maintenance such as adding functionality, correcting latent software defects, etc., over time.

SECTION 3

Software Development Life Cycle: Concept Phase



1 Scope

(1 September 2012) At the beginning of an ISQM software project, there are two paths for developing the software detailed description, see 2/2.3 FIGURE 2. The paths are:

- Design Group (Section 9) delivering Functional Description Documents (FDD).
- Concept Phase (Section 3) delivering a Concept of Operation Document (ConOps) followed by Requirements and Design Phase (Section 4) delivering the SRS and SDS documents.

If the control system functions (code) meet the following requirements, then proceeding using the Design Group and producing the FDD is acceptable to ABS:

i) The control system software to be provided to control or monitor the equipment, control system or integrated system is to be comprised of approximately 85% or more utilizing established functions and code modules or code with the remainder being configuration modifications and/or new code to meet the requirements or specifications.

And

ii) The control system software is to be currently in use within the industry.

a) Multiple updates or modifications that have been made to the control system software over time does not preclude the use of this section and is acceptable to ABS.

Or

iii) Special consideration from ABS is granted.

If the control system software meets the above requirements, see Section 9.

Below are the requirements and recommendations for the Concept Phase with the major deliverable being the ConOps.

The goal of the Concept Phase is to define the integrated system with sufficient detail to facilitate safety review(s), Integrity Level assessments, and identify selected components of the integrated system. The objective of the Concept Phase is to complete a Concept of Operations document (ConOps) which contains the needed architecture, standards, descriptions and requirements that are used by the System Integrator (SI) to begin the Requirements and Design (RD) Phase. Refer to Appendix 1 for activities and requirements for this phase. The Owner may request input from the SI or SBI, as needed, for the development of the ConOps.

The goal of the Concept Phase is to define the integrated system within the ConOps in sufficient detail to:

i) Identify functions and provide traceability of the functions for use in the SDLC.

ii) Incorporate recommendations from safety reviews, if applicable, to the functions description and ConOps.

iii) Assign Integrity Levels to the functions.

iv) Identify integrated system components.

v) Define alarm management philosophy.

It is recommended that functions, activities and deliverables in the latter phases of the SDLC be traceable to the ConOps. Descriptions of the functions and the interfaces definition are a significant portion of the ConOps along with Suppliers' packages data.

During this phase the Integrity Levels (IL) are assigned to the functions and carry this IL assignment to the Software Modules, refer to 3/5. Components of the integrated system, Human Machine Interfaces (HMI) and integrated system's suppliers connected packages are identified.

1.1 Concept Phase Activities *(1 September 2012)*

Verification scenarios for the ISQM integrated system are to be defined in the ConOps to the extent the scenarios are known.

Derived with reference to IEEE 12207-1-2008 Second edition, 2008-02-01, IEEE *Systems and software engineering – Software life cycle processes*, these activities correspond to the scope and objectives of the Concept phase are:

1.1.1 Concept Phase Development

The SI's, Owner's or SBI software development processes are to be mapped to the *ISQM Guide's* SDLC process.

Design tradeoffs, identification and resolutions of (integrated system to suppliers) conflicts are documented. Many decisions made to resolve conflicts will impact the RD Phase. Incorporated standards used, safety, security and human factors are documented. It is recommended that the documents that result from the analysis of the above factors are to be put under configuration management.

A canonical integration model provides the common basis for communication among the associated packages in the integrated system. A canonical integration model benefits the involved parties in identifying integration issues and determining solutions.

i) It is recommended that the SI define a canonical integration model to be used throughout the project and provide the canonical integration model to all stakeholders and Suppliers at the beginning of the Concept Phase.

1.1.2 Systems Requirements Analysis

It is recommended that SI perform the systems requirements analysis. The system requirements analysis is an activity for the development of the ConOps. The system requirements analysis focuses on the determination of integration system requirements and the associated tradeoffs. These specifications describe:

a) These specifications describe:

- ***i)*** Functional requirements, capabilities of the overall system;
- ***ii)*** Accessibility
- ***iii)*** Reliability
- ***iv)*** Maintenance
- ***v)*** Safety

b) Additional considerations for Accessibility, Reliability, Maintenance and Safety (ARMS or RAMS) are:

- ***i)*** Security
- ***ii)*** Human-factors engineering interface requirements
- ***iii)*** Design constraints
- ***iv)*** Qualification requirements.

c) System integration requirements are to be evaluated using:

- ***i)*** Traceability
- ***ii)*** Consistency
- ***iii)*** Testability
- ***iv)*** Feasibility of operations and maintenance (ARMS)

1.1.3 System Integration Architectural Design

The system integration architectural design is an activity for the development of the ConOps. The system integration architectural design activity results in the creation of the top-level architecture of the system. This architecture identifies and facilitates grouping. The recommended groups are:

- ***i)*** Hardware
- ***ii)*** Software
- ***iii)*** Manual operation items.

It is recommended that all software requirements are to be shown on a traceability matrix.

1.1.3(a) System Integration Architecture Evaluation Criteria. The recommended system integration architecture evaluation criteria are:

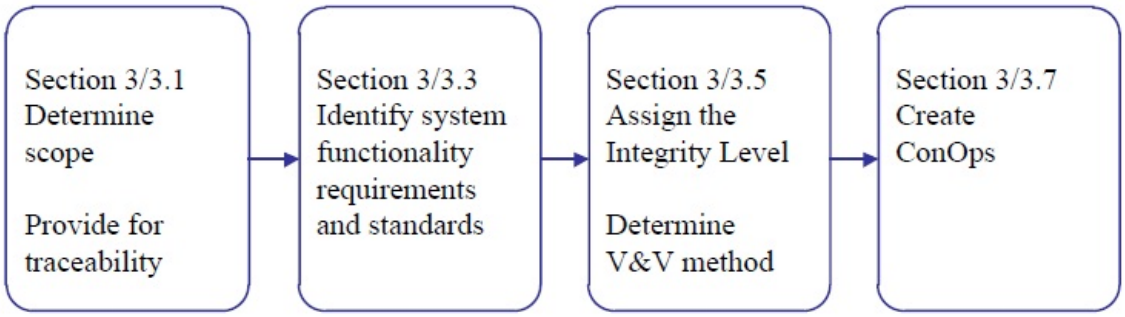
- ***i)*** Traceability
- ***ii)*** Consistency
- ***iii)*** Appropriateness
- ***iv)*** Feasibility

1.3 Concept Phase Organizations Activities

Each organization has assigned activities to facilitate successful completion of this phase. The Concept Phase activities for all organizations are listed in Appendix 1.

3 Example Concept Phase Process Flow for ISQM

FIGURE 1
General Flow of Work During the Concept Phase *(1 September 2012)*



3.1 Scope and Magnitude *(1 September 2012)*

The limitations and boundaries of the integrated system are defined to include any interfaces with hardware and infrastructure components. Traceability is introduced in the software development process via function identification.

i) Issues related to functions are to be identified and traceable through all SDLC phases and safety reviews.

ii) The Owner, with input from the DCO is to state the purpose and scope of the integrated system in the ConOps.

3.3 Identify Functionality of Functions

Each computer-based controlled or monitored package, unit or device is to be identified with a method to allow for tracking of the function. Determine the standards to be used for this project and document the standards to be used.

3.5 Integrity Level Assignment

Refer to 3/5, “Risk Management”, for Integrity Level (IL) assignments. An Integrity Level number is assigned to every function assigned to the ISQM control system. The IL assignment provides for enhanced visibility based on the criticality of the function and may add additional verification scenarios.

3.7 Write Concept of Operations Documents (ConOps)

Refer to Appendix 3 for an example ConOps Table of Contents.

5 Risk Management *(1 September 2012)*

A safety review is to be performed on the defined functions to facilitate identification of important functions such as essential, and safety functions. The techniques used in ANSI/ISA-84 and IEC61508 process may be used for the assessment of Integrity Level (IL), if desired. The safety review may be combined with other safety or operability reviews, hardware FMEA, or software FMECA.

5.1 Safety Reviews and New Technology

5.1.1 SIS Safety Systems

SIS Safety systems, integrated or not, are to follow ANSI/ISA-84 or IEC61508 for assessment of the Safety Integrity Level (SIL).

i) When ANSI/ISA-84 or IEC61508 are used for safety systems, the IL assessment does not apply to the SIS functions.

ii) The *ISQM Guide* does not specify a process for the assignment of the SIL (as per IEC61508 or ANSI/ISA-84) or IL (per ISQM) numbers. The Owner is to choose a logical and recognized process or standard to assign the IL numbers.

5.1.2 Safety Review

Safety review(s) are to be performed on the integrated system and associated packages, units and connected instrumentation.

It is recommended that SI, Owner, DCO, IA, SBI and ABS be present during the safety reviews.

5.1.3 ConOps Reviews

i) SI, IA and the DCO are to review the ConOps. Review comments and accepted recommendations are to be documented. If the SI developed the ConOps then the Owner, IA and DCO are to review the ConOps. Review period as per contract or other agreement with the contracting party.

ii) Comments of the reviews are to be submitted to ABS.

5.1.4 New or Unproven Technology

New or unproven technology carries additional risk. Refer to the ABS *Guidance Notes on Novel Concepts* and the ABS *Guidance Notes on Risk Assessment Applications for the Marine and Offshore Industries* for additional information. The new or novel technologies may be hardware, mechanical equipment, interface protocol or the Software Module coding.

i) New or novel essential systems or essential functions are to be assigned a minimum Integrity Level of IL2.

ii) New or novel SIS functions are to be assigned the minimum Integrity Level of IL3.

iii) New or novel non-essential systems and non SIS functions are to be assigned a minimum Integrity Level of IL1.

5.3 Integrity Level (IL) assessment

The Integrity Level (IL) is assessed by evaluating the consequences of a failure of the function. The Integrity Level represents how important a function is to the operation of the system. The IL number represents the degree of confidence the Owner and/or DCO desires for the function to operate as specified including fail safe state(s). IL numbers are assigned by Owner, with input from the DCO and SI, being attentive to the requirements of national and international authorities and classification societies.

The Integrity Level derives from the desired confidence of performance and severity of failure consequence. The IL assessment is based upon:

i) Safety consequences

ii) Environmental consequences

iii) Business impact (optional)

5.3.1

Functions are to be rated in Safety and Environmental categories. Business impact is optional.

- Business impact is optional and will not be reviewed by ABS. It is recommended that business impact be included in the IL assessment.

Potential safety and environmental consequences are to be considered when assessing functions for IL assignment. Integrity Level assignment may be increased due to company's risk tolerance and for potential business impact.

5.3.2

There are four Integrity Levels (IL). Each carries increasingly more severe consequences from IL0, which is considered as having little to no impact on safety, environment or business outcomes, to IL3 which could have significant or severe consequences affecting safety, the environment or business issues. The ISQM control system carries the number of the highest IL rated software function. A control system with IL0 to IL2 functions and a single IL3 software function is assigned an overall rating of IL3. It is not recommended to assign IL3 rating to all functions within the ISQM control system unless the risk analysis indicates this rating for the other functions.

5.3.3

Essential systems and functions

i) Essential systems and functions are assigned IL2 or IL3. Essential systems may be assigned an IL1 rating with justification, redundancy, etc., provided to ABS for special consideration.

ii) SIS systems are to be IL3, as SIS is defined by IEC61508 or ANSI/ISA 84, IMO and optional assignment by Owner to non-SIS functions or systems. SIS systems may be assigned an IL2 with justification, redundancy, etc., provided to ABS for special consideration.

iii) Refer to 4-9-3/7.1 of the *Marine Vessel Rules* for additional guidance.

iv) ESD systems utilizing software functions are to be IL3. ESD systems maybe assigned an IL2 with justification, redundancy, etc. provided to ABS for special consideration.

An implementation of the IL assignment in the Concept Phase allows for scrutiny of the individual functions and the system as a whole. The goal is to provide a more reliable and stable integrated system. The risks include schedule, obsolescence of hardware and/or software and reliability (quality) of the software development. The IL assignment conveys to the Software module (code) of the function.

5.3.4

The overall IL number of the integrated system is to equal the highest IL number assigned to any of the functions controlled by the ISQM control system.

TABLE 1
Integrity Level Table *(1 September 2012)*

IL	*Potential Consequences*			*Examples, not inclusive*
	Safety	*Environmental*	*Business*	
0	Negligible	Negligible	Minor impact on operation. Might affect supporting process system but not main process system.	Entertainment System, Administrative computer systems, office network, Data Collection system (non-Authority required)
1	Might eventually lead to marginal safety incident	Might eventually lead to a marginal environmental incident	Might lead to maintenance shutdown of non-critical system. Main process continues to operate.	Non-essential control of systems, BPCS, Non-essential communication systems, Vessel Management System. New or unproven non-essential technologies minimum rating.
2	Within a short time could cause critical injury, lost time, accident or loss of a life.	Critical environmental impact	Shutdown of main system, excessive time for repair.	Drilling control system, BPCS, SIS systems (minimum rating), PMS, essential systems, DP control system, main engine control system, safety systems, new or unproven essential technologies minimum rating.
3	Immediate and Catastrophic lost time injuries, or multiple loss of life.	Catastrophic environmental impact	Significant repair time or loss of the marine or offshore asset.	Drilling Blowout Preventer control system, SIS or safety control systems, boiler firing control system, etc.

Catastrophic: Loss of human life, loss of asset, loss of system safety or security, or extensive financial or social loss.
Critical: Permanent injury or multiple lost time injuries, mission critical system damage, or significant financial or social loss.
Marginal: Lost time injury or illness, degradation of ship or units performance, or some financial or social loss.
Negligible: First aid injury or illness, non-mission critical system(s) shutdown or degraded, or DCO inconvenience.

5.3.5

Owner and DCO are to provide criteria used for IL assessment of the functions to ABS. Owner and DCO may refine terms as used above to fit company's risk tolerance.

5.5 IL Assignment Functions Documentation Requirements

5.5.1 IL0

Generally, control and monitoring of non-essential and relatively unimportant functions. Monitoring of important or essential functions where the information is not used by DCO's personnel to make essential decisions and where the data is not used in algorithms (Software Modules) for safety, important, and essential Software Modules.

i) Descriptions of the operational or normal condition (not required for degraded or failed conditions) of the functions are to be specified in the ConOps or FDD.

ii) The data displayed on an HMI for the DCO to make essential or important decisions are not IL0. This may apply to drilling operations where human experience and knowledge is used for the safe operation of the process.

iii) Interface description

Requirement for ARMS: Specify the requirement for testing, repair and restarting without interference with the redundant running system.

5.5.2 IL1

Generally monitoring and/or control of non-essential functions:

i) Descriptions of the normal (operational) condition, of the function are to be specified in the ConOps or FDD.

ii) Descriptions of the failed condition (Failure state(s)) are to be specified in the ConOps or FDD

iii) Interface description

iv) Requirement for ARMS. Specify the requirement for testing, repair and restarting without interference with the redundant running system.

v) If system is redundant, specify the requirement for testing, repair and restarting without interference with the redundant operating component or part.

vi) Obsolescence risks are defined and option selected for ARMS with replacement component(s) or part(s).

5.5.3 IL2

Essential and important systems and functions:

i) Descriptions of the normal, condition of the functions are to be specified in the ConOps or FDD.

ii) Descriptions of the degraded condition (state) of the functions are to be specified in the ConOps or FDD.

iii) Descriptions of the failed condition (Failure state(s)) are to be specified in the ConOps or FDD.

iv) Interface description

v) Requirement for ARMS. Specify the requirement for testing, repair and restarting without interference with the redundant running system.

vi) Specify the requirement for testing, repair and restarting without interference with the redundant operating component or part.

vii) Obsolescence risks are defined and option selected for ARMS with replacement component(s) or part(s).

5.5.4 IL3

Essential, SIS, and important systems and functions:

i) Descriptions of the normal, condition requirements are to be specified in the ConOps or FDD.

ii) Descriptions of the degraded condition (state) of the functions are to be specified in the ConOps or FDD.

iii) Descriptions of the failed condition (Failure state(s)) are to be specified in the ConOps or FDD.

iv) Interface description

v) Requirement for ARMS. Specify the requirement for testing, repair and restarting without interference with the redundant running system.

vi) Specify the requirement for testing, repair and restarting without interference with the redundant operating component or part.

vii) Obsolescence risks are defined and option selected for ARMS with replacement component(s) or part(s).

5.5.5

Refer to 3/5.5 TABLE 2 for recommended overall control system IL assignments.

TABLE 2
Recommended Safety and Environmental Overall Control System IL Assignments *(1 September 2012)*

Control System	*Description*	*IL0*	*IL1*	*IL2*	*IL3*	*Notes and Recommendations*
Acoustic BOP control	Fixed and/or portable unit(s)	N/A	N/A	Note 1	X	
Acoustic DP input		N/A	X	X	N/A	
Ballast Control System		N/A	X	X	Note 1	
Ballast Water Treatment		X	X	Note 1	N/A	
BOP	Blow Out Preventer. Includes Diverter and Choke and Kill functions	N/A	N/A	Note 1	X	All Functions
Cement Pump		N/A	X	Note 1	N/A	
Chemical, gas or oil processing or separation system		N/A	X	X	Note 1	
Drawworks		N/A	Note 1	X	Note 3	ESD Functions only
Drilling Control System		N/A	Note 1	X	Note 3	See Note 3
Drilling Heave Control	Drawworks or active heave compensation lifting appliances	N/A	X	X	Note 1	
Drilling Power System	Drilling Variable Frequency Drives, Switchboards, etc.	N/A	X	X	N/A	
Drilling Top Drive		X	X	Note 1	N/A	
Dual Fuel Engine Fuel System		N/A	Note 1	X	Note 1	
Dynamic Positioning		N/A	Note 1	X	N/A	
EDS	Emergency Disconnect	N/A	N/A	X	X	
Engine Control System		N/A	X	Note 1	N/A	
ESD	Emergency Shutdown	N/A	N/A	Note 1	X	See Note 2
Fire and Gas		N/A	N/A	Note 1	X	All Functions
Fixed Rig Power Management	Jack ups, or any anchored asset	N/A	X	X	N/A	
Fuel Treatment		N/A	X	X	Note 1	

Control System	*Description*	*IL0*	*IL1*	*IL2*	*IL3*	*Notes and Recommendations*
Governor		N/A	X	Note 1	N/A	
Horizontal Pipe Handling System		N/A	X	X	N/A	
Ice Load Monitoring		N/A	X	X	Note 1	
Lifting Appliances	Braking function, Hoisting and Lowering function, and Heave Compensation function, non drawworks functions	N/A	Note 1	X	N/A	
LNG Refrigeration		N/A	Note 1	X	Note 1	
Marine Riser System	Includes Riser Tensioner	N/A	X	X	Note 1	
Mud Monitoring Control System	Low pressure system	N/A	X	Note 1	N/A	
Mud Pumps	High pressure system	N/A	X	Note 1	N/A	
Process Safety System (SIS)	IEC 61508, ISA 84	N/A	N/A	Note 1	X	All Functions
Production Subsea ESD		N/A	N/A	Note 1	X	
Production Subsea monitoring	Includes pressure, temperature and flow, hydrate, wax, etc.	Note 1	X	Note 1	N/A	
Thruster		N/A	Note 1	X	N/A	
Vertical Pipe Handling System		N/A	X	X	N/A	
Vessel Management		N/A	X	X	N/A	
Vessel Power Management		N/A	Note 1	X	N/A	
Vessel Stability		N/A	X	X	N/A	
Zone Monitoring System		N/A	X	X	Note 1	

Notes:

1) Contact ABS for special consideration with justification to have this rating

2) If the control system contains emergency shutdown (ESD) functions, these functions are to be rated IL2 or IL3 based upon consequences of a failure to the crew or asset and the environment. Many systems have separate and independent ESD systems that allow the Owner to lower the IL rating of the ISQM control system. The BOP (choke and kill) is considered the backup for the drilling control system and mud control system.

3) The simplex software initiated ESD functions located within the Drilling Control System are IL3 if the functions are simplex. If the software initiated ESD functions are redundant, i.e. located within other control systems or hardwired, recommend IL2. It is recommended that other functions within the Drilling Control System are IL2 or less.

N/A: Not available. ABS may not agree to offer a notation for the chosen control system based on the overall IL rating. Contact ABS

X Available selection without contacting ABS

5.7 Software Quality Management

The Owner is to specify the verification method to be followed. There are three options of verification of the integrated system software. In the V V & T Phase, the software for the system, at a minimum, is to

operate as specified in the SRS and SDS or FDD (verification). It is permissible to use all three methods of verification where the Owner selected method is to verify the IL2 and IL3 functions, where feasible.

i) *Closed Loop:* ABS to specially consider this option

ii) *Software-In-the-Loop:* The integrated system software is executed on a non-native platform and the simulation may reside on the same machine

iii) *Hardware-In-the-Loop:* The integrated system software is executed on its native platform and the simulation is running on a separate machine of different technology

The selection of the verification method is to include considerations of complexity of the functions and associated Software Modules, the functions' Integrity Level and the quantity of supplier's packages to integrate. The development of the simulation is performed in parallel with the integrated system software development and not at the conclusion of the software development.

Refer to Section 6 for a description of the V & V methods.

5.9 Obsolescence Plans

5.9.1

The SI is to provide a high-level hardware obsolescence plan for the integrated system. Accessibility, Reliability, Maintenance and Safety (ARMS) are to be considered when developing the plan.

5.9.2

The SI is to provide a high-level software obsolescence plan for the integrated system software.

7 Concept of Operations Document (ConOps) *(1 September 2012)*

An example ConOps Table of Contents is provided in Appendix 3. The ConOps is to be reviewed by the Owner (if not developed by the Owner), SBI, DCO, SI (if not developed by the SI), IA, and ABS. The ConOps is to contain the information listed in 3/7.1. Review period as per contract or other agreement with the contracting party.

7.1 General Topics

i) Overall scope and goals of the project

ii) Supplier's packages, if applicable

- ***a)*** Manufacturer or the SI's or Supplier's part number
- ***b)*** Model Number, if possible
- ***c)*** Interface protocol
- ***d)*** Constraints

iii) Function's description including:

- ***a)*** Sufficient detail to develop the RD Phase documents.
  - Integrator may have input on the word "sufficiently". For common and well understood functions, the detail could be "sufficient" with a one line statement.
- ***b)*** Every function is to have a description and an assigned Integrity Level (IL0 to IL3).
- ***c)*** Fail safe state(s).

iv) Number and description of Human Machine Interfaces to include:

- ***a)*** Manufacturer

b) Model Number or the SI's or Supplier's part number, if possible

c) Interface protocol

d) Constraints

v) Number and description of interfaces (data collection, SCADA systems…):

a) Quantity of network or direct connections to the ISQM control system

b) Interface protocol of interfaced network, control system and/or equipment

c) Constraints of interfaced network, control system and/or equipment

vi) Primary verification method

7.3 Definition of the Project Scope

The Owner, with input from DCO, is to state the purpose and scope of the integrated system in the ConOps.

7.5 Integrated System Major Components and boundary

7.5.1

Major packages or components are to be preliminarily selected at a high Integrity Level.

Note:

At this point in the process, the SI and/or Owner know what interfaced or connected equipment packages from other vendors is needed to meet the ConOps. The Dynamic Positioning System will interface with the Power Management System from Vendor Xyz, as an example. A listing of the interfaced or connected equipment and the HMIs are included in the ConOps.

7.5.2

Control System component redundancy is not to lower the Integrity Level of the function if the redundant control system is running identical software. This includes the integrated system and the connected components. If there is a defect in the software, the function and the associated connected component or equipment under control may fail as both the primary and backup control systems are running identical code.

7.5.3

It is permissible to lower the IL number if the redundancy consists of two different technologies (i.e., PLC control and another means of control or controlled shutdown, mechanical, hydraulic, etc.).

7.7 Constraints

Constraints are to be identified and delineated in the Concept of Operations document. These can include:

i) Supplier's package limitations,

ii) Existing, new or novel technologies to be applied

iii) Software limitation, if known

iv) Network or serial communications limitations of the Supplier's package (function), if known

v) Anticipated software function risk assessment

Example: The Supplier's package may only be able to communicate using Modbus at 9600 BPS leading to the need for additional hardware module(s) for the integrated system. The process control group may suggest advanced control using unproven Software Modules (fuzzy logic, model predictive control) but the risk is judged too high by the Owner leading to using simpler proven control.

7.7.1

Suppliers' constraints are to be mitigated as necessary.

7.7.2

Supplier's verification report (V&V Report) for IL1, IL2 and IL3 ISQM control system connected packages are provided and any exceptions are noted in the FDD. Verification IL2 and IL3 functions are to be witnessed by ABS and the V&V Report may not be available at the time of FDD development.

Note:

The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL1, IL2 and IL3 systems to begin construction.

7.7.3

Supplier's verification plan (V&V Plan) is to be provided for IL2 or IL3 ISQM control system packages and any exceptions are noted in the FDD.

Note:

The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL2 and IL3 systems to begin construction.

9 Deliverables

The deliverable is the Concept of Operations phase document (ConOps).

11 Milestones *(1 September 2012)*

11.1 Concept Phase Complete, Milestone M2

The M2 Milestone signifies that:

i) Components of the integrated system are identified.

ii) Safety review report(s) are submitted.

iii) The ConOps has been updated with safety review(s), FMEA, etc. accepted recommendations.

iv) Integrity Levels are assigned to all functions.

v) Management of Change procedure (MOC) is applied to the ConOps.

vi) Potential subcontractors have been consulted.

vii) Selection of the primary V & V method for the ISQM control system

viii) Supplier's V & V Plans are provided for IL2 or IL3 ISQM control system packages, exceptions are noted in the ConOps

Note:

The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL2 and IL3 systems to begin construction.

ix) Supplier's V & V Reports, for IL1 ISQM control system connected packages are provided, exceptions are noted in the ConOps. Verification IL2 and IL3 functions are to be witnessed by ABS and the V & V Report may not be available at the time of ConOps development.

Note:

The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL2 and IL3 systems to begin construction.

x) Updated integrated system's project and overall schedules are complete.

xi) Hardware and software obsolescence plans are included in the ConOps.

xii) ARMS considerations are noted in the ConOps.

xiii) Design considerations tradeoffs are complete and included in the ConOps.

xiv) ConOps has been reviewed by DCO, SI, IA, and ABS. Review period as per contract or other agreement with the contracting party.

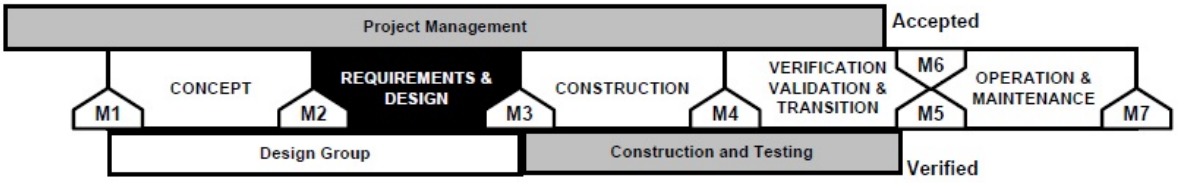
xv) List of connected supplier's equipment.

11.3 Authorization from the Owner to Proceed to the RD Phase

The Owner and ABS, with input from the IA, are to approve the ConOps to proceed to the RD Phase.

SECTION 4

Software Development Life Cycle: Requirements and Design (RD) Phase



1 Scope and Objectives

(1 September 2012) At the beginning of an ISQM software project, there are two paths for developing the software detailed description, see 2/2.3 FIGURE 2. The paths are:

- Design Group (Section 9) delivering Functional Description Documents (FDD).
- Concept Phase (3) delivering a Concept of Operation Document (ConOps) followed by Requirements and Design Phase (4) delivering the SRS and SDS documents.

If the control system functions (code) meet the following requirements, then proceeding using the Design Group and producing the FDD is acceptable to ABS:

i) The control system software to be provided to control or monitor the equipment, control system or integrated system is to be comprised of approximately 85% or more utilizing established functions and code modules or code with the remainder being configuration modifications and/or new code to meet the requirements or specifications.

And

ii) The control system software is to be currently in use within the industry.

a) Multiple updates or modifications that have been made to the control system software over time does not preclude the use of this section and is acceptable to ABS.

Or

iii) Special consideration from ABS is granted.

If the control system software meets the above requirements, see Section 9.

Below are the requirements and recommendations for the Requirements and Design Phase with the major deliverables being the SRS and SDS.

1.1 General

The Requirements and Design (RD) Phase refines the Concept of Operations document (ConOps). The focus of the RD Phase is the specification, architecture, and design of the integrated control software. The RD Phase uses the ConOps to provide guidance regarding system features. In concert with principles and quality criteria which are finalized early in the RD Phase, these ConOps inputs serve as guiding criteria for the specification, architecture, and the detailed design of the software. The resulting RD Phase documents are the basis of the Construction phase. Refer to Appendix 1 for activities and requirements for this phase.

If any new constraints are identified, they are to be documented and discussed with the Owner. Mitigation of the constraints are documented and the ConOps updated per the Management of Change (MOC) procedure. RD Phase documents are reviewed against the ConOps and, upon the Owner's approval, become the verification acceptance documents.

1.3 RD Phase Activities

(1 September 2012) During the RD Phase, focus shifts from system level description and designs to software level specification, architecture and design. From these artifacts, programmers (coders) are eventually able to convert modeled relationships and flows into software code. The two activities that are called out in IEEE 12207 that map to the scope and objectives of the RD Phase are below as well as the two documents developed during this phase:

1.3.1 Software Requirements Analysis *(1 September 2012)*

In software requirements analysis, the functions are de-composed into software modules. For purposes of software configuration management in the support processes, each identified software module is a configuration item. Software module's specification contains functional capability and performance specifics. Other factors for consideration are: interfaces external to the Software Module, qualification requirements, safety and environmental specifications, especially those involved in operations and maintenance, security requirements, human factors (ergonomics), user documentation, operation and maintenance requirements.

1.3.2 Software Architectural Design

1.3.2(a) During the software architectural design activity, the SI:

i) Transforms software requirements into a top-level architecture that identifies software components for each of the software modules.

ii) Assigns each of the requirements in the SRS to one or more Software Module(s).

iii) Documents requirements and Software Modules in the traceability matrices (Refer to Appendix 3).

iv) Documents the architecture of the Software Modules.

v) Develops:

- Top-level external interface designs,
- Top-level design for any database,
- The preliminary design of the user documents
- Preliminary test requirements.

1.3.2(b) It is recommended that the software architectural design be evaluated using the criteria recommended in the IEEE 12207 standard:

i) Traceability to the requirements of the software item

ii) External consistency with the requirements of the software item

iii) Internal consistency between software components

iv) Appropriateness of design methods and standards used

v) Feasibility of detailed design

vi) Feasibility of operations and maintenance

1.3.3 Software Requirement Specification (SRS) *(1 September 2012)*

The ISQM SRS is a specification for the integration of a defined set of functions consisting of particular software products, programs, or set of programs that perform defined functions in a defined environment. The SRS is to be reviewed by the Owner, DCO, IA organizations and ABS. Review period as per contract or other agreement with the contracting party. The SI is to have the discretion to include or not include software functional proprietary information or intellectual property of the SI in the SRS. The SI is to describe the functions in descriptive terms.

The SRS is to address the following, at a minimum:

i) *Functionality:* Describe, in high-level terms, the purpose of the control system and software.

ii) *External interfaces:* Describe, in high-level descriptive terms, how the software provides for interaction with users (user interfaces), the system execution hardware, externally interfaced system support hardware, and externally interfaced system support software.

iii) *Performance:* Describe the availability of the control systems, scan speed if fast enough for the application, recovery or reboot time.

iv) *Attributes:* Describe, in high-level descriptive terms, the reusability of the code, the maintainability, security, etc., considerations.

v) *Design constraints:* Describe the constraints imposed on this implementation.

vi) *Other:* Describe the standards that are applied to the implementation of the software, execution hardware, software language used in the implementation, policies for database integrity, resource limits, operating environment(s) etc.

1.3.4 Software Design Specification (SDS) *(1 September 2012)*

The ISQM integrated SDS describes the design of the system's integrated components. Typical contents include system or component architecture, control logic, data structures, input/output formats, interface descriptions, and algorithms. The SDS is to be reviewed by the Owner, DCO, IA organizations and ABS. Review period as per contract or other agreement with the contracting party. The SI is to have the discretion to include or not include software functional proprietary information or intellectual property of the SI in the SDS. The SI is to describe the functions in descriptive terms. Review period as per contract or other agreement with the contracting party.

1.3.4(a) Integrated Software Detailed Design Process. Software detail design begins in the RD Phase and continues in the Construction Phase. Software integration detailed design is the activity where software component integration of the Software Modules are refined into lower levels comprised of software integration units that will be coded in the Construction Phase. These detailed design specifications are developed during the RD Phase and refined during the Construction Phase so that the SI developers (coders) have a clear understanding of the precise nature of the task the software is to accomplish.

1.3.4(b) The software detailed design and test requirements are to be evaluated using these criteria recommended in the IEEE 12207 standard:

i) Traceability to the requirements of the software item

ii) External consistency with the architectural design

iii) Internal consistency between software components (modules, programs)

iv) Appropriateness of design methods and standards used

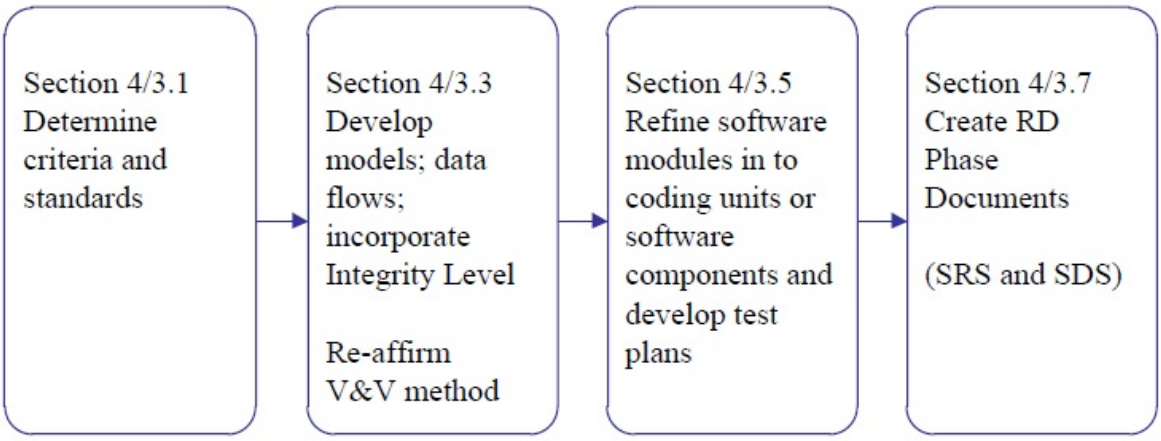
v) Feasibility testing

vi) Feasibility of operations and maintenance

3 Example RD Phase Design Process Flow for ISQM

4/3 FIGURE 1 is a nominal depiction of a sequence that could be used to arrive at the RD Phase Documents.

FIGURE 1
General Flow of Work During the Requirements and Design Phase *(1 September 2012)*



3.1 Criteria and Standards Selection *(1 September 2012)*

The criteria and standards are established and agreed to by the Owner and DCO organizations in step 3.1. While developing the software architecture, the assigned Integrity Levels are to be incorporated as well as the approved Owner-specified primary verification method.

3.3 Models

It is recommended that the SI develop models, data flows and other graphical support items, as needed. Refer to Appendix 4 for example models.

3.5 Identify Coding Units and Test Plans

Decomposition of Software Modules is accomplished. Identification of coding units and test plan development are completed.

3.7 RD Documents

The SRS and SDS sections of the Requirements and Design Phase document are developed.

5 Requirements and Design Phase Documents

The RD Phase documents consist of the Software Requirements Specification (SRS) and the Software Design Specification (SDS).

5.1 Software Requirements Specification (SRS)

An example SRS Table of Contents is provided in Appendix 4. The SRS, at a minimum, is to contain:

i) The results of the software requirements analysis activity

ii) Work Process flow Diagrams

iii) Criteria and Standards

iv) The Software Modules with associated functions are de-constructed into sub-software modules which make up the required function

v) Preliminary test requirements

vi) Functional test requirements

vii) Top-level external interface specifications

viii) Functions are traceable to the ConOps

5.3 Software Design Specification (SDS) *(1 September 2012)*

An example SDS Table of Contents is provided in Appendix 4. The SDS, at a minimum, is to contain:

i) Top-level design for any database

ii) Design for internal and external interfaces

iii) Preliminary design of the user documents

iv) Software architecture design evaluation

v) Software design constraints

vi) Functions are traceable to the ConOps

5.5 Risk Management

At this point, there are two main aspects for risks, project and operational.

5.5.1 Project Risk Management *(1 September 2012)*

It is recommended that metrics be collected, measured and managed during the RD and Construction Phases to notify the Project Manager of potential issues with schedule, effort, and software quality. Recommended metrics are listed in Appendix 8. The metrics data is for the SI's internal use to manage their software quality.

5.5.2 Operational Risk Management

Operational risks are addressed with the safety reviews, Failure Mode, Effect and Criticality Analysis (FMECA) and other reviews. New technology may come to light during the RD Phase.

5.5.3 Supplier's Package Documentation

Supplier's package documentation is to be considered in the overall plan.

5.5.4 Software Control System FMECA *(1 September 2012)*

The purpose of the FMECA is to determine that a single Software Module failure will not lead to failures of other Software Modules or loss of the control system.

i) IL2 and IL3 assigned ISQM control systems are to have a software focused functional FMECA performed.

ii) A Control System FMECA is to provide traceability of the Software Modules to the relevant functions in the Traceability Matrix.

iii) A Control System FMECA of IL2 and IL3 functions is to be performed including interfaces with integrated control systems that may have an effect upon the function.

iv) Update the SRS and SDS or FDD with FMECA recommendations.

5.5.5 New or Unproven Technology

New or unproven technology carries additional risk. ABS has Guidance Notes on risk assessment, *Guidance Notes on Review and Approval of Novel Concepts*, to assist the user. The new or novel technologies may be hardware, mechanical equipment, interface protocol or the Software Module coding. Refer to 3/5.1.4

5.5.6 New Functionality Added in the RD Phase

i) The Owner is to update the ConOps.

ii) Safety reviews of the new functions are to be conducted and the results are to be documented.

iii) If the function was added after the Software Control System FMECA, a FMECA is to be conducted to address any risks with the new functions and associated Software Modules.

5.7 Document Approval *(1 September 2012)*

The SRS and SDS are to be reviewed by the Owner, DCO, IA organizations and ABS for consistency with the ConOps. Review period as per contract or other agreement with the contracting party.

i) The SI is to update and approve the SRS and SDS per the Control System FMECA and comments from reviews.

5.9 Function Requirements for ConOps with IL assignment

5.9.1 General requirements for all Functions

i) Unique identification of the functions for traceability

ii) Functional description

iii) IL assignment number

iv) Identify function as Essential or SIS function

v) Safety review(s) traceability or cross reference

vi) Interface requirement(s) of the function's equipment

vii) Process conditions

- Temperature, pressure
- Operating ranges
- Alarm points

viii) If function is a COTS

- Supplier's identification (Model number)
- Interface requirements
- Constraints

ix) Verification scenarios

- Refer to Section 6, Figures 2 through 5 for V & V Plan requirements

7 V & V activities during the RD Phase

The V & V organization is to develop a draft of the V & V Plan.

9 RD Phase Deliverables

i) The Software Requirements Specifications (SRS) and Software Design Specifications (SDS).

ii) Initial V & V Plan developed by the V & V Organization.

iii) Variance of standards report, if variance occurred.

11 RD Phase Complete, Milestone M3

It is recognized that some RD phase activities extend into the Construction Phase.

M3 Milestone: RD Phase complete

i) Interface or integration between components of the integrated systems is clearly defined.

ii) Detailed descriptions of functional components are complete.

iii) Alignment of the SRS and SDS with the ConOps phase document has been accomplished

iv) Integrity Levels align per the concept scope

v) Update software and overall project schedule

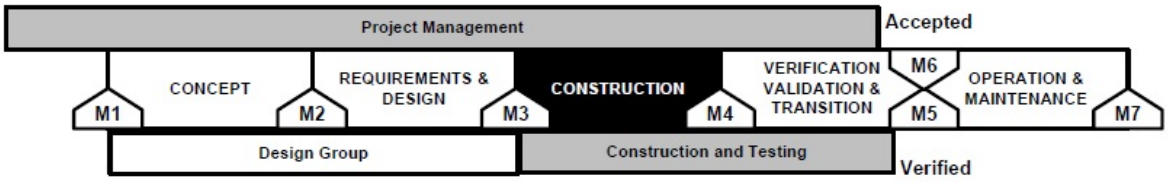
vi) Authorization from the Owner to proceed to the Construction Phase.

vii) Variance of standards report(s).

viii) Issue the SDS and SRS (Issue for Construction)

SECTION 5

Software Development Life Cycle: Construction Phase



1 Scope and Objectives *(1 September 2012)*

The RD Phase provided the technical plans for the system requirements for software in the SRS and SDS or the FDD. The Construction Phase develops and implements the integration code of the functions that executes the SRS, SDS, FDD and other requirements. Refer to Appendix 1 for activities and requirements for this phase.

The Construction Phase consists of the SRS and SDS or FDD refinements, coding of the Software Modules, integration of COTS products' configuration, unit testing, integration testing, and software system level acceptance testing is performed in the Construction Phase.

The following is to be managed during the Construction Phase by the System Integrator:

i) SRS and SDS or FDD errors or clarifications identified in the SRS and SDS or FDD are to be corrected, reviewed and approved by Owner before code is written.

ii) The SI is to provide a document attesting that all SI developed Software Modules have been reviewed and unit tested by the SI.

iii) Once units of integrated Software Modules are reviewed, they are to be placed under configuration management and integrated into the baseline project.

iv) After all individual Software Modules have been successfully incorporated, an overall software system level SI integration test is to be performed to verify that the software satisfies the requirements of the SRS and SDS or FDD.

v) It is recommended that the Owner and/or DCO perform periodic reviews of the SI's and/or contractor's software development. ABS is to be notified of these reviews.

vi) It is recommended that integration testing be performed each time a Software Module is integrated into the baseline to verify that it interfaces correctly with the remainder of the software.

vii) At the completion of the Construction Phase, the SI is to provide a test summary report.

1.1 Construction Phase Activities

The three activities that are called out in IEEE 12207 that map to the scope and objectives of the Construction Phase are:

i) Software development and testing

ii) Software integration

iii) Software SI integration testing

1.1.1 Software Coding and Testing

This activity consists of developing custom Software Modules and the use of library modules, integration of COTS products, and interfaces. The SI completes the software architecture using the models, diagrams and functional specifications, SRS and SDS or FDD. The programmer, working with the SRS and SDS or the FDD, translates specifications into the Software Modules' code and establishes the sequencing of software development. SI's internal testing of the individual Software Module is then performed.

1.1.1(a) Peer reviews of the integrated Software Modules code is to be performed by a SI programmer who is not involved in the project for IL2 & IL3 assigned functions. Peer reviewer is to use a standard method verifying that the integrated Software Modules code is:

i) *Correct:* It has traceability to the SRS and SDS or FDD.

ii) *Complete:* There is no missing functionality.

iii) *Coherent:* The logic is clear and not unnecessarily complex.

iv) *Maintainable:* Source code logic is easy to read and is well commented. For COTS configuration, clear notes have been written on the integration, registers and configuration(s) made.

v) *Efficient:* there are no unacceptable performance bottlenecks

1.1.1(b) It is recommended that during the final detailed design, coding and unit/database testing, the SI is to consider the following and document the result of the evaluation:

i) Traceability to the requirements and design of the software item

ii) Consistency with the requirements and design of the software item

iii) Consistency between unit requirements, canonical integration model

iv) Test coverage of units

v) Feasibility of software integration and testing

vi) Feasibility of operation and maintenance

1.1.2 Software Integration

This activity develops the integration plan which details the levels of integration testing that are to be accomplished. The purpose of this test planning is that the developed code conforms to the requirements, architecture and specifications developed in this and earlier phases, refer to Appendix 6 for an example V & V Plan Table of Contents. The integration plan is a section of the V & V Plan.

i) It is recommended that the integration plan includes test requirements, procedures, data, responsibilities and schedule.

ii) Each requirement is to be supported by a set of tests, test cases and test procedures for the integration testing.

iii) Each test case is to be documented and traceable to the requirement(s) in the SRS and SDS or FDD.

1.1.2(a) The SI is to evaluate the integration plan, test results and user documentation using the following criteria:

i) Traceability to the system requirements

ii) Consistency with the system requirements

iii) Consistency between unit requirements

iv) Test coverage of the requirements of the software item

v) Appropriateness of test standards and methods used

vi) Conformance to expected results

vii) Feasibility of software qualification testing

viii) Feasibility of operation and maintenance

1.1.3 Software SI Integration Testing

It is recommended that the SI test every Software Module, internally, against the SRS and SDS or FDD requirements (functional and integration requirements) through peer reviews or other methods.

It is recommended that the software detailed design and test requirements be evaluated using the following criteria:

i) Test coverage of the requirements of the software item

ii) Conformance to expected results

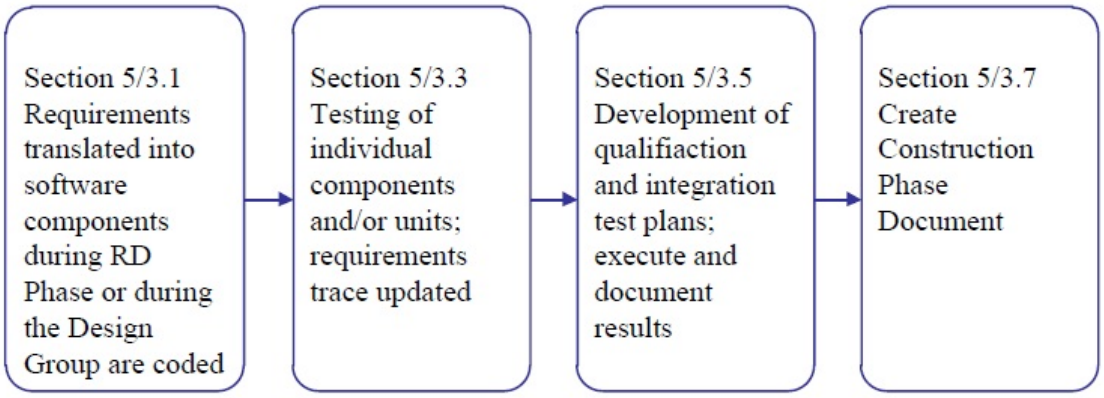
iii) Feasibility of software acceptance testing

iv) Feasibility of operation and maintenance

3 Example Construction Phase Process Flow for ISQM

5/3 FIGURE 1 is a nominal depiction of a sequence that could be used to arrive at the completion of the construction phase

FIGURE 1
General Flow of Work During the Construction Phase *(1 September 2012)*



3.1 Requirements Translated and Coded

Based on the functional specifications and artifacts, the programmer updates the detailed integration specifications (per the MOC policy) and writes the code that fulfills those requirements and specifications.

3.3 Components Tested

The programmer performs basic tests (abnormal end, unit, compiling) at the Software Module level on the code that has been written.

3.5 Integration Plans

Integration testing between software modules is performed; some COTS integration testing may be possible; results are to be documented for IL2 and IL3 assigned functions.

3.7 Creating Construction Document *(1 September 2012)*

The SRS and SDS or FDD sections of the Requirements and Design phase document are updated. At approximately 90% of the coding completed, as determined by the SI, reissue the updated SRS and SDS or FDD.

5 Construction Phase Document

The following deliverables are included in the Construction Phase documents: detailed code specifications and the results of the unit testing for IL2 and IL3 assigned functions, the integration plan and the overall integrated system test results.

5.1 General Topics

i) *(1 September 2012)* Coding specifications and location of the actual compiled software (the actual code is not contained in the document). The code is to be maintained under configuration management by the SI according to the SI's MOC policy.

ii) Consolidated report of test plans results, including unit, integration and qualification test results.

iii) Conclusions/recommendations for any further actions based on the test results.

5.3 Risk Management

Managing risks involve project and operational risks.

5.3.1 Project Risk Management *(1 September 2012)*

It is recommended that metrics be collected. The recommended metrics are listed in Appendix 8.

5.3.2 Operational Risk Management

Operational risk are addressed with the safety reviews, FMECA and reviews conducted earlier in the process. New technology may come to light during the Construction Phase.

5.3.3 Software Control System FMECA

i) A Control System FMECA is to provide traceability of the Software Modules to the relevant functions in the Traceability Matrix.

ii) A Control System FMECA is to be performed on the integrated system as a whole for functions changed during the Construction Phase.

iii) A Control System FMECA of IL2 and IL3 functions is to be performed for functions changed during the Construction Phase.

5.3.4 New or Unproven Technology

New or unproven technology carries additional risk. ABS has guidance notes on risk assessment, *Guidance Notes on Review and Approval of Novel Concepts* to assist the user. The new or novel

technologies may be hardware, mechanical equipment, interface protocol or the Software Module coding. Refer to 3/5.1.4

5.5 Document Approval *(1 September 2012)*

Updates to ConOps, SRS and SDS or FDD are to be reviewed by Owner, DCO, IA organizations and ABS. ConOps or FDD is to be accepted by the Owner. Consolidated test results are to be reviewed by Owner, DCO, and IA organizations. Review period is per contract or other arrangements with contracting party.

7 V & V Activities during the Construction Phase

The V & V Organization is to perform the following activities during the Construction Phase:

i) The V & V organization is to detail the V & V Plan during the Construction Phase

ii) The V & V Plan is to be peer reviewed by the V & V Organization.

iii) V & V Organization is to configure the simulator during the Construction Phase. Refer to Section 6.

iv) Program the simulator

v) Validate the simulator program

7.1 V & V Reviews *(1 September 2012)*

i) The Owner, DCO, SI, IA, and ABS are to review the V&V Plan. Review period as per contract or other agreement with the contracting party.

ii) Provide consolidated V & V Plan report of the reviews.

9 Construction Phase Deliverables *(1 September 2012)*

The following are the deliverables of the Construction Phase:

i) Consolidated report of test plans results. IL2 and IL3 results are to be included.

ii) Completed, integrated Software Module code.

iii) Updated V & V Plan by Verification Organization.

iv) Updated ConOps or FDD has been issued.

v) Updated SRS and SDS or FDD has been issued.

11 Construction Phase Complete, Milestone M4 *(1 September 2012)*

M4 Milestone: Construction Phase complete

i) Code development is complete.

ii) Integration and SI testing complete.

iii) Alignment of the test results with the functional test strategy and plans have been reviewed and verified against traceability matrices.

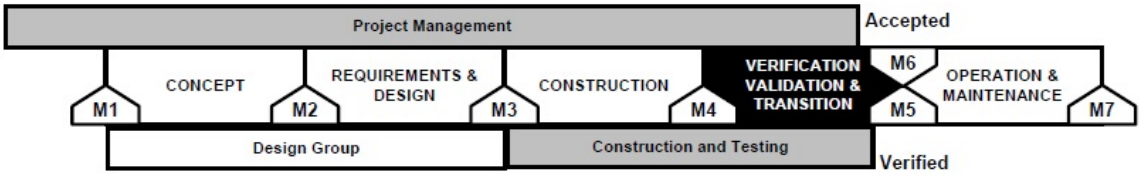
iv) SI releases the integrated system programming for the Verification, Validation and Transition Phase.

v) V & V Plan is complete. (Developed by the V & V Organization)

vi) Simulation is complete (validated by the V & V Organization)

SECTION 6

Software Development Life Cycle: Verification, Validation and Transition Phase



1 Scope *(1 September 2012)*

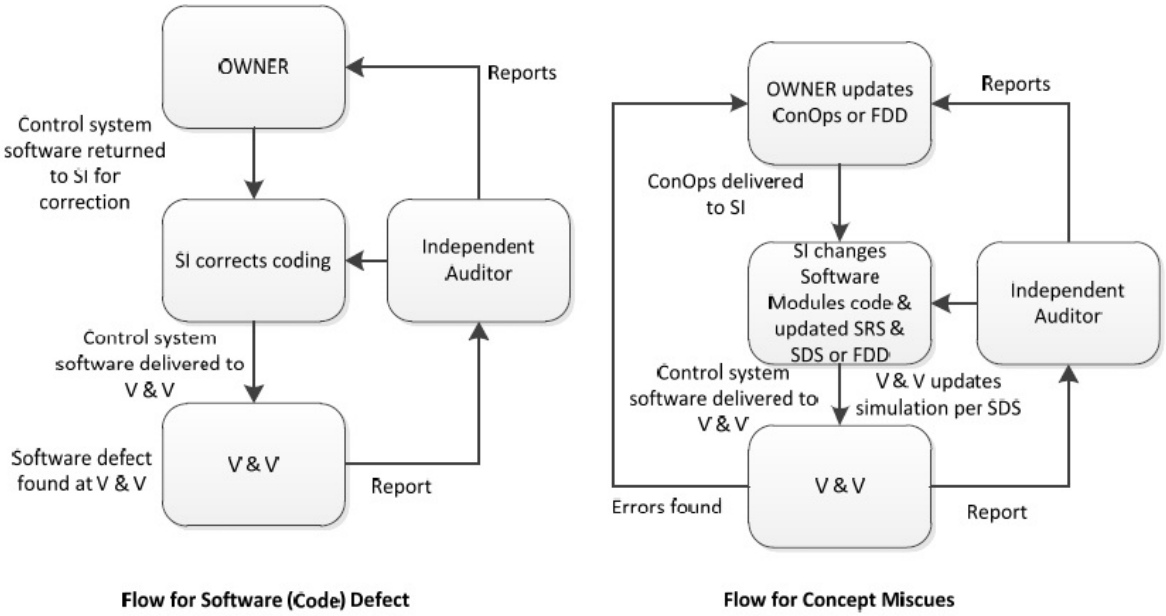
The V V & T Phase, the control system software is verified to the SRS and SDS or FDD. This process is iterative and regressive to detect any new defect introduced by the correction of a previously detected and corrected defect(s). The control system is validated during commissioning and sea trials and with a review of the control system's performance compared against the current ConOps. Interactions of hardware and software components are to be considered when testing the software in the V&V Plan. Refer to Appendix 1 for activities and requirements for this phase.

The V&V organization is to develop a plan (V&V Plan) for verification of the control system software based upon the requirements listed in the SRS and SDS or FDD.

The V&V Organization is to generate a V&V Report listing the defects, errors or other anomalies discovered (functions that failed to perform) and concept errors observed by Owner, DCO or the Independent Auditor. It is recommended that the Owner and/or DCO witness the verification testing. Once the integrated system software has passed the verification, the software is to be "locked", per the SI'sMOC policy, to prevent changes and possible introduction of new defects.

The validation of the control system occurs when the Owner agrees that the control system software performs per the current ConOps.

FIGURE 1
Software and Reporting Flow during the V V & T Phase *(1 September 2012)*



1.1 Review of V&V Report

Owner and DCO are to review the V&V Report to identify any concept errors and resolve them. The SI is to correct coding defects. ABS is to review the V&V Report. Review period as per contract or other agreement with the contracting party.

1.3 Scan for Viruses and other Malicious Software Prior to Verification Activities

V&V Organization is to run a virus scan on the control system software before any V&V activities. Report to Owner, DCO, SI and ABS the results of the scan.

i) The V&V Organization is to state that they are utilizing the most recent virus definition available for their virus scanning program.

ii) Provide virus definition number or identifier in the virus scan report.

iii) The SI is to state if the SI's compiled software is known to contain scripts that are detected by the virus scanning program as potentially malicious.

- ***a)*** The SI is to provide the name or type of malicious software that the script(s) detected (as spyware, Trojan, etc.) and the number of instances reported. This facilitates identification of potentially other malicious software in the O&M Phase.

iv) If the SI, Supplier or Sub-suppliers provide antivirus software with their control system, any conflicts with the Owners security plan are to be resolved between the Owner and the SI, Supplier or Sub-supplier.

- ***a)*** If antivirus software is installed on the control system, then it is recommended that the SI, supplier or sub-supplier provide details on how and when the virus definition is updated onboard.

1.5 V&V Review of the Simulation

The simulator is to include connected components data (monitoring and control) commands to and from the integrated system, signals, software interlocks and alarms, as necessary, to verify the integrated system's code and clearly demonstrate the control system software to the stakeholders as specified in the SRS and SDS or FDD.

The simulation is to be of sufficient fidelity, to include real world dynamic systems and effects, to the extent reasonable, to verify the integrated system's code. The V&V Organization is to document the results of the verification.

Note:

Reasonable is defined as providing enough fidelity to test the control system software functions and programming while providing enough feedback to the V&V Organization that the software is functioning per the SRS and SDS or the FDD. Reasonable is determined by the V&V Organization with input from the SI.

1.5.1 V&V Peer Review of the Simulation

Prior to the verification the simulation configuration is to be peer reviewed by the V&V organization for:

i) Traceability to the requirements using the current traceability matrix.

ii) Feasibility of the simulation

iii) Provide a report to the SBI, Owner and ABS.

3 Objective *(1 September 2012)*

A V&V process facilitates an objective assessment of the integrated system. The V&V process demonstrates the control system software and its conformance to the V&V Plan (SRS and SDS or FDD) and generates V&V Report(s) of the detected defects and errors.

5 V V&T Methods *(1 September 2012)*

The primary verification method was selected in the Concept Phase. Below is a further discussion of each method. There are three options of software verification, closed loop (specially considered), Software-In-the-Loop and Hardware-In-the-Loop verification. The minimum goal of the V V&T phase is to verify the software performs as specified in the SRS and SDS or FDD. The simulation is to have sufficient fidelity to test the control system software.

The simulation is to include connected components' data (monitoring and control), commands to and from the integrated system, signals, software interlocks and alarms, as necessary, to verify the integrated system's code and clearly demonstrate the control system software to the stakeholders as specified in the SRS and SDS or FDD. The intent is to verify the integrated control system, not necessarily the software of the connected components.

5.1 Closed Loop Verification

The inputs and outputs of the computer-based integrated system are simulated with minimal interaction of the other integrated components. Closed Loop verification may require changing register values of the program to evaluate the integrated system software response. A comprehensive understanding of the software code and its functions are required and this limits the application to simple systems. Special consideration and prior approval from ABS is required prior to selecting Closed Loop Verification. SI and Owner/DCO are to provide documentation that these closed loop verification requirement are met.

5.1.1 Requirements for the Closed Loop Verification Method:

i) Simple integrated or stand alone computer-based systems.

ii) Three or fewer integrated components

iii) A small number of complex functions and their associated complex software modules.

iv) No essential or safety functions are controlled by the integrated system. If essential or safety functions are monitored on the system and this data is used for human decision making then Closed Loop testing may not be appropriate.

v) IL1 functions will not lead to safety or environmental consequences.

vi) No IL2 or IL3 functions exist on the system.

5.3 Software-In-The-Loop Verification

The control system software is being executed on non-native hardware and the simulation is being executed on the same or a separate computer. The simulation is to be of sufficient fidelity, to include real world dynamic systems, to the extent required, to verify the integrated system's code and documenting the results of the stimulus. Fidelity of the simulation is to be sufficient to allow for verification of the control system software to current SRS and SDS or FDD.

5.5 Hardware-In-The-Loop Verification

The integrated system's program is running on its native hardware (CPU) with interface cards for communication with available components and the simulation computer and the control system's backplane.

The simulator is running on separate computer hardware connected to the control system's interface cards. The simulator supports emulating the components of the integrated system. The simulation is to be of sufficient fidelity, to include real world dynamic systems, to the extent required, to verify the integrated system's code and documenting the results of the stimulus. Fidelity of the simulation is to be sufficient to allow for verification of the control system software to the current SRS and SDS or FDD.

7 Defect Ranking

(1 September 2012) The SI with input from the V&V, Owner or IA Organizations determines if the deficiency is a control system code defect, simulation code defect or a concept error.

TABLE 1
Defect Categories *(1 September 2012)*

Defect Term	*Description*	*Rank*
Critical	These are the extremely severe defects, which have already halted or are capable of halting the operation of the computer-based control system. Critical defects are also defects that are capable of unsafe operation of the Equipment Under Control (EUC). All Critical defects are to be corrected and the control system retested.	4
Major	These are severe defects, which have not halted the system, but have seriously degraded the performance, caused unintended action or incorrect data transmitted. There exists no acceptable (to Owner and DCO) workarounds. All Major defects are to be corrected and the control system retested.	3

Defect Term	*Description*	*Rank*
Moderate	Major Defects which have an acceptable (to Owner & DCO) workaround. Such defects may result in data latency but not in essential or IL2 or IL3 functions. The integrated system and the function continues to operate, although with a failure. Such a disruption or non-availability of some functionality may be acceptable for a limited period of time for IL1 functions. Moderate defects could cause corruption of some non-critical data values in a way that is tolerable for a short period. Changes to the Operating Manual may be called a Moderate Defect. The Owner is to review the impact and risk of such a change. When a Moderate Defect is detected on an IL2 or IL3 assigned functions, The SI is to facilitate a safety review on the proposed workaround involving the Owner, DCO and SI organizations. ABS is to be notified of the safety review meeting. Provide report of the safety review to the IA and ABS. It is recommended that safety reviews be performed on IL0 and IL1 functions.	2
Minor	Defects which can or have caused a low-level disruption of function(s). Such defects may result in data latency but not in essential, safety or IL2 or IL3 functions. The integrated system and the function continue to operate, although with a failure. Such a disruption or non-availability of some functionality may be acceptable for a limited period of time for IL1 functions. Minor defects could cause corruption of some noncritical data values in a way that is tolerable for a short period. Essential or SIS functions assigned IL2 or IL3 assigned functions are to be corrected Non-essential and non SIS IL2 or IL3 assigned functions are to be corrected at the Owner's option. IL0 or IL1 assigned functions are to be corrected at the Owner's option.	1
Cosmetic	These types of defects are the ones, which are primarily related to the presentation or the layout of the data. However there is no danger of corruption of data and incorrect values. If essential or safety functions are monitored on the system and this data is used for human decision making then Cosmetic ranking may not be appropriate. Depending upon the IL rating of the function, the Software Module may be released with the permission of the Owner and DCO. HMI graphic colors may not be a Cosmetic Defect.	0

Regulatory Authorities (IMO, IACS, and National) requirements may raise Defect Category.

7.1 Integrity Level and Defect Category

7/7.1 TABLE 2 contains requirement and recommendations for defect or error remediation.

TABLE 2
IL Ranking and Defect Category, Requirements and Recommendations *(1 September 2012)*
Owner may Require Defect Correction

IL Ranking	*Defect Category*	*Requirements and Recommendations*
0	0	Correction may be delayed
0	1	Correction may be delayed
0	2	Correction may be delayed
0	3	Requires correcting and retesting
0	4	Requires correcting and retesting
1	0	Correction may be delayed

IL Ranking	*Defect Category*	*Requirements and Recommendations*
1	1	Correction may be delayed
1	2	Correction may be delayed. Owner and DCO to review consequences and risks
1	3	Requires correcting and retesting
1	4	Requires correcting and retesting
2	0	Requires correcting and retesting if Essential function, May be delayed if IL consequence(s) are business related only. On non-Essential functions, Owner and DCO to review consequences and risks
2	1	Requires correcting and retesting if Essential function, May be delayed if IL consequence(s) are business related only. On non-Essential functions, Owner and DCO to review consequences and risks
2	2	Requires correcting and retesting if Essential function, May be delayed if IL consequence(s) are business related only. On non-Essential functions, Owner and DCO to review consequences and risks
2	3	Requires correcting and retesting
2	4	Requires correcting and retesting
3	0	Requires correcting and retesting if Essential function, May be delayed if IL consequence(s) are business related only. On non-Essential functions, Owner and DCO to review consequences and risks
3	1	Requires correcting and retesting
3	2	Requires correcting and retesting
3	3	Requires correcting and retesting
3	4	Requires correcting and retesting

9 V&V Plan *(1 September 2012)*

The V&V Plan follows from the V&V requirements in the current SRS and SDS or FDD. Refer to Appendix 6 for an example V&V Plan.

9.1 V&V Plan Description

The V&V Plan describes the purpose, goals, and scope of the software V&V effort. The plan is to follow the requirements listed in the current SRS and SDS or FDD.

i) Satisfy standards, practices and conventions.

ii) Scenarios are to be traceable to the current SRS and SDS or FDD.

iii) V & V Plan is to include a process to collect supportive evidence that the software satisfies software system requirements.

iv) It is recommended that the ConOps be reviewed to facilitate understanding the intent of the requirements listed in the current SRS and SDS or FDD. Section 6, Figures 2 through Figure 5 provide guidance for verification activities based on the assigned IL level.

v) The V & V Plan is the documentation that specifies the scope, approach, resources, and schedule of testing activities.

vi) Test designs are the documentation that specifies the details of the test approach for a Software Modules.

vii) V & V Plan is the documentation that specifies a sequence of actions for the execution of a test.

viii) Document results and generate the V&V Report.

FIGURE 2
IL0 Verification Process Diagram

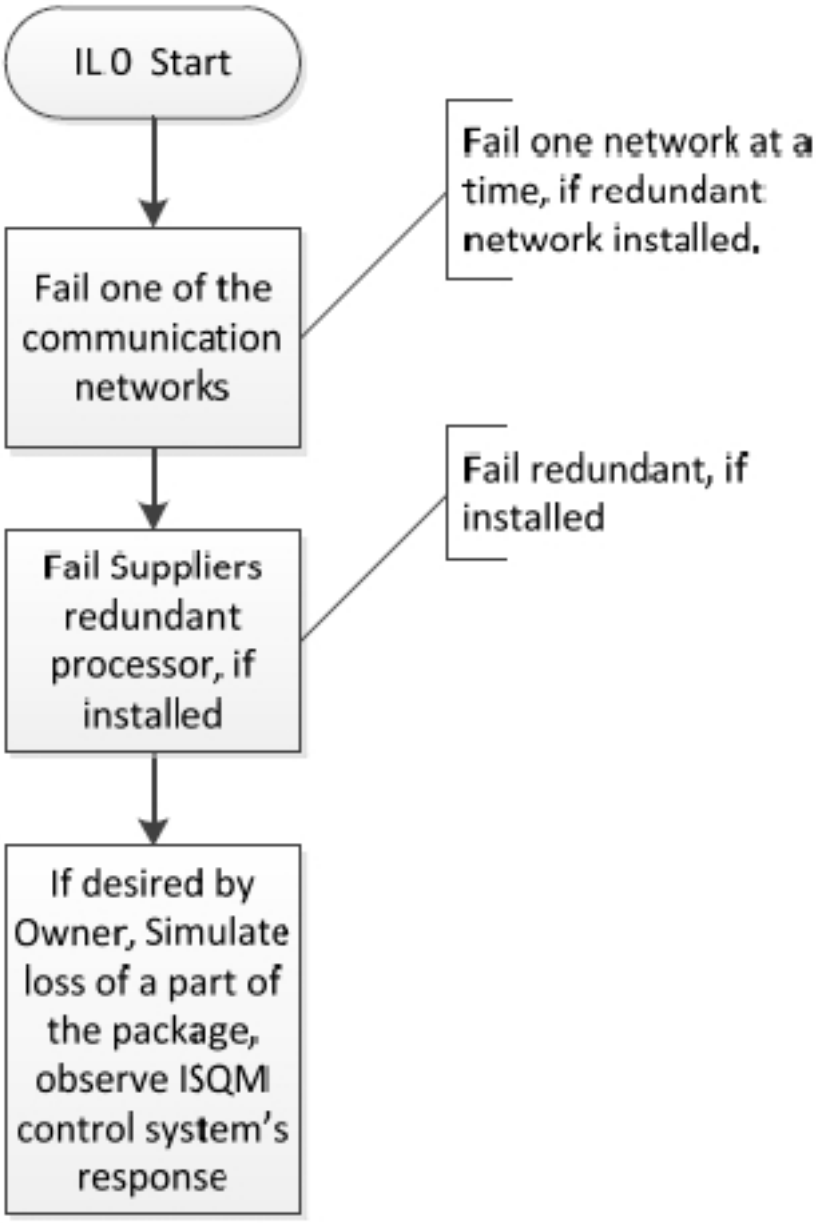


FIGURE 3
IL1 Verification Process Diagram

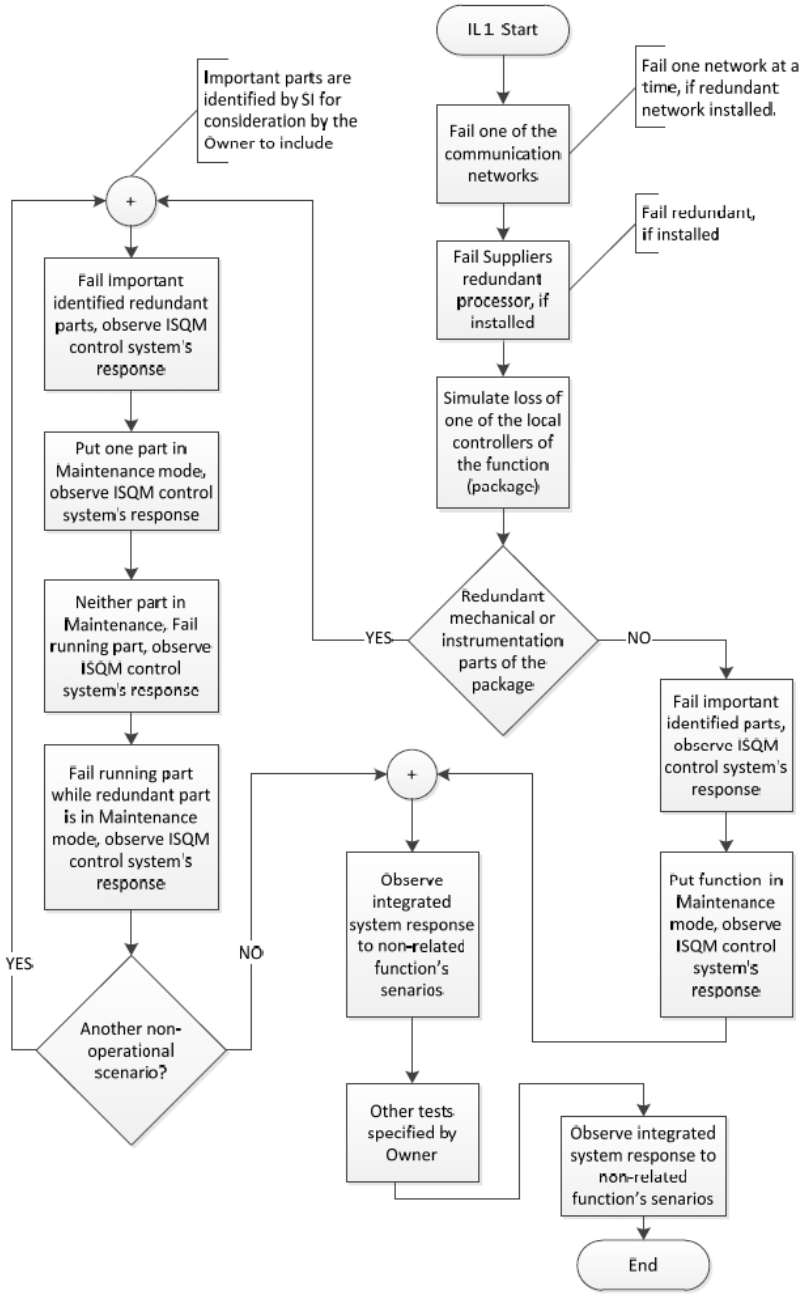


FIGURE 4
IL2 Verification Process Diagram *(1 September 2012)*

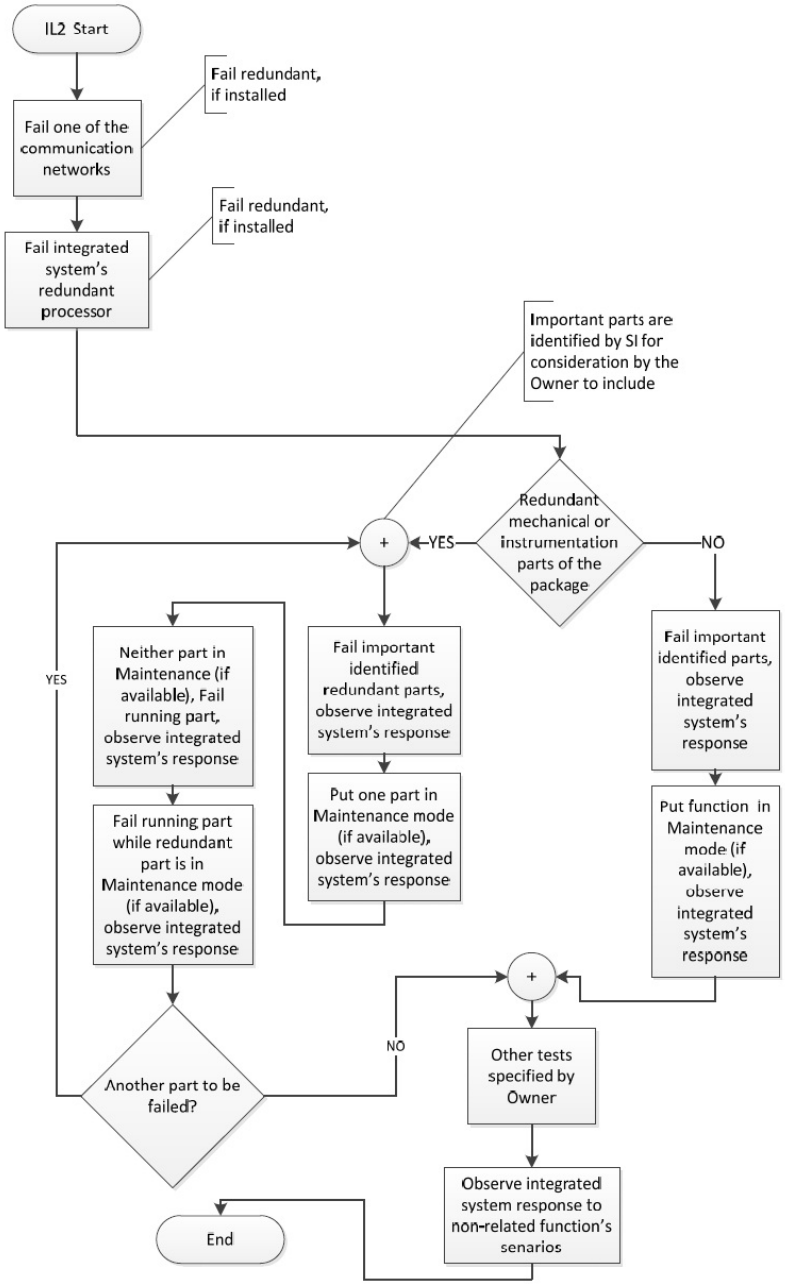


FIGURE 5
IL3 Verification Process Diagram *(1 September 2012)*

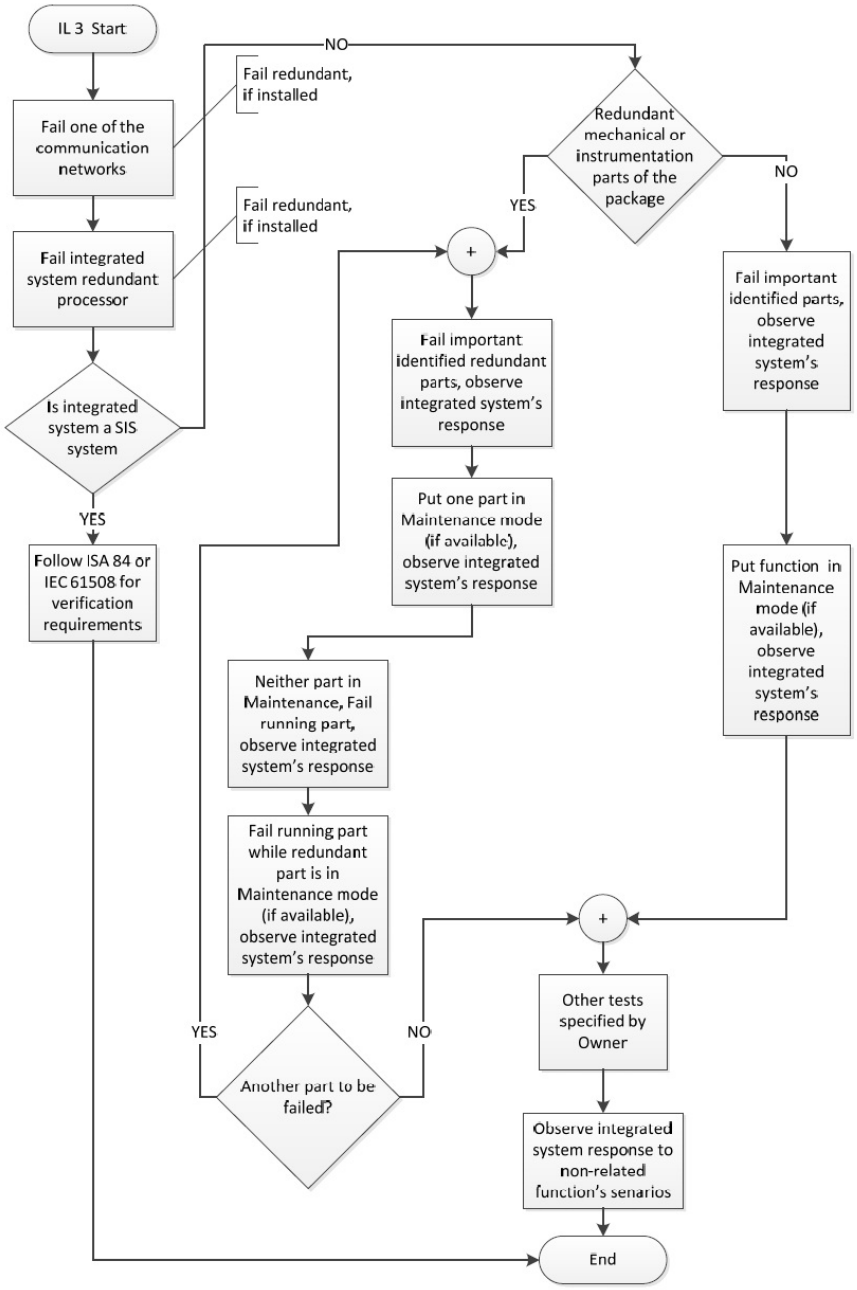
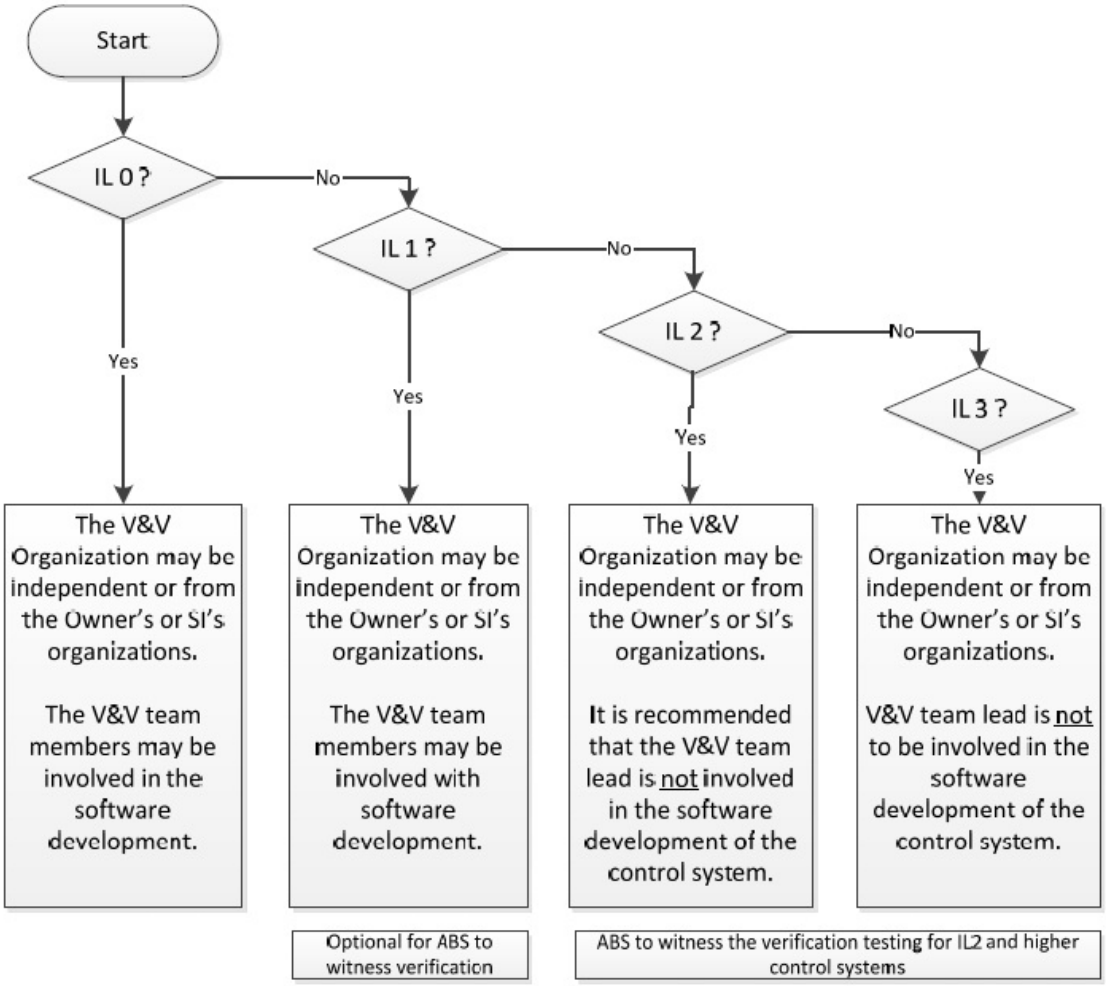


FIGURE 6
V&V Organizations Independence from SI Organization by IL Assignment *(1 September 2012)*



9.3 V&V Plan Approval

The Owner, DCO, IA, and the SI organizations and ABS are to review the V&V Plan. The Owner and ABS, with input from the IA, are to approve the V&V Plan with comments from the reviewers. Review period as per contract or other agreement with the contracting party.

11 Verification and Validation Report (V&V Report) *(1 September 2012)*

The report is generated by the V&V Organization using traceable notation on the pass or fail of each function described in the current SRS and SDS or FDD. This report is to include:

i) Anomalies discovered in the Software Modules.

ii) Cause of the defects, errors or anomaly, if known

iii) Impact of defects, errors or anomaly on the function and if it affected other functions.

iv) The simulation designs, simulation scenarios, simulation procedures and simulation results.

v) Deviations from the V&V Plan. To include function identifier, what is deviated from and why there was a deviation.

vi) Recommendations

11.1 V&V Report Reviews

The interim and final V&V Reports are to be reviewed by the Owner, DCO, SI, IA organizations and ABS.

13 System Integrator's Operation and Maintenance (O & M) Plan and Operating Manual *(1 September 2012)*

i) The Owner is to develop an O&M Plan. Refer to Section 7 for details.

ii) The SI is to develop the Operating Manual(s).

15 V V&T Phase, Verification Accepted, Milestone M5 *(1 September 2012)*

i) Verification has been completed. The control system software meets the requirements per the current SRS and SDS or FDD.

ii) V&V Report is completed and delivered to stakeholder.

iii) Software has been scanned for viruses after Verification is complete and before shipping the software by the SI or the V&V. Refer to 7/1.3 for requirements.

iv) Owner's O&M Plan is developed.

v) Owner accepts verified control system software.

17 Deliverables *(1 September 2012)*

i) Consolidated V&V Report summary

ii) The simulation peer review report.

iii) The Owner is to develop an O & M Plan. Refer to Section 7.

iv) The SI is to develop the Operating Manual(s).

19 V V&T Phase, Validation and Acceptance, Milestone M6 *(1 September 2012)*

i) Owner validates the software as meeting the current ConOps. This includes concept changes over the course of the project.

ii) All the components and subsystems perform as defined in the updated ConOps.

iii) Operating Manuals are delivered.

iv) SBI, Owner, DCO and/or SI is to update the Vessel Software Registry.

v) SBI, Owner, DCO and/or SI is to update the Control Equipment Registry.

vi) Commissioning tests.

vii) Authorization from the Owner to proceed to the O & M Phase.

21 Transition *(1 September 2012)*

During the transition, the DCO is taking responsibility of the operation and maintenance of the control system. The SI is to pass the final documentation to the DCO and Owner or as specified in the contract.

i) Associated ISQM documentation (manuals, ConOps, SRS and SDS, or FDD etc.) is to be delivered to the Owner and DCO.

ii) The change management of the software is to follow the Owner's or DCO's MOC procedure for approval of installation. The SI is to maintain their change management for the software updates internally to the SI Organization. The Owner/DCO allows installation of the new or updated software per their MOC.

21.1 Operations and Maintenance Plan (O&M Plan)

21.1.1 Review of O&M Plan

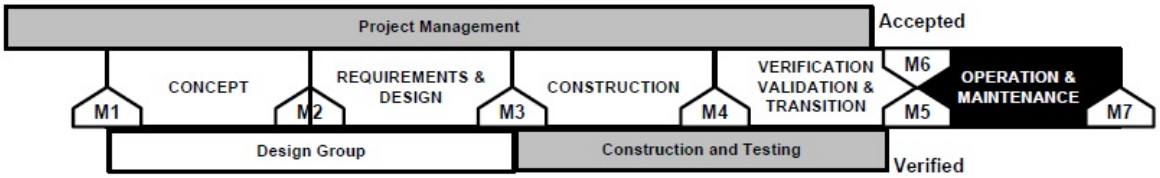
It is recommended that the O&M Plan is reviewed by the DCO. The SI is to provide documentation (Operations manual, etc.) for inclusion in the O&M Plan by the Owner or DCO.

i) It is recommended that the control system software be included in the training of the DCO's staff

ii) It is recommended that the Owner or DCO is to identify an IT Maintenance Manager. Refer to Appendix 7 for list of responsibilities.

SECTION 7

Software Development Life Cycle: Operation and Maintenance Phase



1 Scope *(1 September 2012)*

This phase covers all operational and maintenance activities, including scheduled and unscheduled upgrades and problem resolution activities. The phase also extends to retirement activities of the ISQM control system. The activities of this phase are the responsibility of the DCO and under the DCO direction, the Supplier(s). After acceptance of the ISQM system, the Owner or the DCO is to provide the Operation and Maintenance Plan with input and documents provided by the SI, Suppliers and Sub-suppliers. Refer to Appendix 7 for an Operation and Maintenance Plan template. Refer to Appendix 1 for activities and requirements for this phase.

1.1 Scan for Viruses and other Malicious Software

Prior to installation, all artifacts, software code, executables and the physical medium used for installation on the vessel are to be scanned for viruses and malicious software. Results of the scan are to be documented and kept with the Software Registry. Refer to 6/1.3.

3 Review of the O&M Artifacts *(1 September 2012)*

The following table lists the artifacts created in prior phases, the phase in which they were accepted, the stakeholder and phases in which they were modified. These artifacts are reviewed by listed stakeholder for completeness and as the entry criteria into the O & M Phase. It is recommended that the O & M Phase is not to be initiated if these artifacts are missing or incomplete.

TABLE 1
O & M Phase Artifacts *(1 September 2012)*

Artifact	*Phase Created*	*Phase Accepted*	*Phase Modified*	*Stakeholder*
Control Equipment Registry	Concept	RD	V V&T	DCO
Management of Change Policy	Concept	Concept	N/A	Owner

Artifact	*Phase Created*	*Phase Accepted*	*Phase Modified*	*Stakeholder*
Management of Change Process	Concept	Concept	N/A	Owner
Operations & Maintenance Plan	V V&T	V V&T	V V&T	DCO
Vessel Software Registry	Concept	RD	V V&T	DCO
Software Configuration Management Plan	Concept	Concept	N/A	Owner
Software Change Control Process	Concept	Concept	N/A	Owner

The following Paragraphs describe the minimum information to be included in each artifact.

3.1 Operation & Maintenance Plan (O & M Plan)

i) The Owner and/or DCO is to develop the O&M Plan utilizing documentation from the SI, Suppliers and sub-suppliers, as applicable.

ii) The SI is to provide documentation for the Owner's and DCO's use in operation and maintenance plan, which is to be developed by the Owner or the DCO.

3.1.1 O&M Plan submittals and Activities

i) The O&M Plan identifies the stakeholders who are responsible for operations and maintenance of the system's software.

ii) The plan defines what constitutes operation and maintenance.

iii) The plan identifies where scheduled operation and maintenance occur (e.g., on the asset, in a shipyard, at the vendors manufacturing facility, remotely via a manufacturers' asset network access).

iv) The plan defines when specific operations and maintenance occur; (e.g., scheduled testing of BOP equipment, replacement of obsolete PLCs, and preventative maintenance schedules for connected equipment with control systems).

v) The SI is to recommend training interval and courses for the operation and maintenance of the system. If the SI's recommendation is to contact their local office, then Owner or DCO is to contact the SI's local office to acquire the necessary information.

vi) The plan describes the operation and maintenance activities to be performed (e.g., software backup and restore).

vii) The plan describes the checks to be made and the data to be collected for health and performance monitoring (e.g., preventative maintenance checklists, logging and accounting files' formats, automatic scheduling, recording scripts, alarm recording).

viii) The plan covers schedules for reporting of system health and performance to provide feedback to management on O&M effectiveness.

ix) The plan specifies all documents required (e.g., relevant policy directives, system configuration documentation, and operating & maintenance manuals) that are provided by the SI.

x) The plan addresses system testing and configuration documentation updates following configuration changes, repairs, and upgrades.

xi) The plan addresses expected life and end-of-life replacement, upgrade and retirement as specifically as possible.

xii) It is recommended that the Owner or DCO identifies the personnel resources, facilities, and tools, needed for operation and maintenance (e.g. specialized manufacturer provided tools and test equipment, software test scripts, configuration management tools).

xiii) It is recommended that the Owner identify funding sources and uses for ongoing operation and maintenance.

xiv) The plan is to reference individual safety, security and software/firmware configuration management plans.

xv) The Owner is to add to the list of documents required (e.g., relevant policy directives, system configuration documentation, and operating & maintenance manuals) not provided by the SI.

xvi) The plan addresses reactive maintenance procedures (e.g., lockout/tagout, emergency software patching, remote access for break/fix).

3.3 Owner's Management of Change (MOC) Policy

It is recommended that the DCO review the MOC policy to determine completeness. Refer to Appendix 7 for an example of a recommended process. Records are to be maintained on the vessel for ABS's review. It is recommended that the records also be maintained at a central location. The DCO is to review the Management of Change (MOC) policy for the following requirements and activities, not inclusive, to determine completeness:

i) There is a definition for the various roles and responsibilities within the MOC process for the Owner's Organization. The "initiator" can be anyone within the Owner or DCO's Organizations with the "person in charge" as the final approver.

ii) There is to be a process in place for software verification of changes to IL2 and IL3 components.

iii) It is recommended that there is a defined life cycle to the MOC with reviews and defined milestones.

iv) Change process evaluations are to be part of the process.

v) Formal approval processes are defined.

vi) The Owner's or DCO's MOC is to be followed for new limits and process safety updates. Changes are to be recorded.

vii) Formal vessel or offshore unit notification is to be part of the Owner's or DCO's MOC procedure.

viii) The DCO is to manage software changes within the asset's MOC policy.

ix) The DCO is to notify ABS of IL2 and IL3 functions added, updated or deleted from the ISQM control system.

x) It is recommended that the software changes, updates, deletion or new functionality be reviewed for impact upon the scope of the control system including subsystems.

3.5 Software Registry

The DCO is to maintain the Software Registry for the following considerations, not inclusive, to determine completeness. The Owner and DCO are to physically take possession of the integrated Software Modules created as part of the Construction Phase.

At a minimum, the registry is to contain the following types of sample information:

ID Code	*Description*	*IL #*	*Supplier*	*System*	*Hardware Processor*	*Software Module*	*Version*
101P1	Driller's Control HMI	2	Vendor #1	Server A A20	Dual CPU Server	Server OS	Build 2600
101P2	Embedded Chair A Controller	3	Vendor #4	OpSta PLC A26	PLC	PLC OS	

ID Code	*Description*	*IL #*	*Supplier*	*System*	*Hardware Processor*	*Software Module*	*Version*
102P1	Driller's Control HMI	2	Vendor #1	Server B A21	Quad CPU Server	Server OS	Build 2600
102P2	Embedded Chair B Controller	3	Vendor #2	OpSta PLC A27	PLC	PLC OS	
103P1	Driller's Control HMI	2	Vendor #1	Server C A22	Quad CPU Server	Server OS	Build 2600
103P2	Embedded Chair C Controller	3	Vendor #3	OpSta PLC A28	PLC	PLC OS	
104P1	Driller's Control HMI	2	Vendor #1	Server D A23	Quad CPU Server	Server OS	Build 2600
104P2	Embedded Chair D Controller	3	Vendor #2	OpSta PLC A29	PLC	PLC OS	

3.5.1 Additional Information

Additional information for consideration is:

i) Size of file

ii) Physical Location of the backup, if provided by SI and/or Suppliers

iii) Location of restore procedures for the control system and components, HMI, servers, etc.

iv) Date of last software installation

3.7 Control Equipment Registry

It is recommended that the Owner and DCO review the Control Equipment Registry for the following considerations, not inclusive, to determine completeness. At a minimum, the registry contains the following types of sample information:

ID Code	*Description – Location*	*IL #*	*System*	*Hardware Processor*	*Software OS*	*Software Hosted*
101CE1	SERVER FOR CONTROL CONSOLE – LIR, cabinet V1418	2	Server A A20	Dual CPU Server	Server OS	Driller's Control HMI
101CE2	PLC FOR CONTROL CONSOLE – Drillers cabin, under chair A	3	OpSta PLC A26	PLC	PLC OS	Embedded Chair A Controller
102CE1	SERVER FOR CONTROL CONSOLE – LIR, cabinet V1418	2	Server B A21	Quad CPU Server	Server OS	Driller's Control HMI
102CE2	PLC FOR CONTROL CONSOLE – Drillers cabin, under chair	3	OpSta PLC A27	PLC	PLC OS	Embedded Chair B Controller
103CE1	SERVER FOR CONTROL CONSOLE – LIR ,cabinet V1418	2	Server C A22	Quad CPU Server	Server OS	Driller's Control HMI

ID Code	*Description – Location*	*IL #*	*System*	*Hardware Processor*	*Software OS*	*Software Hosted*
103CE2	PLC FOR CONTROL CONSOLE – Drillers cabin, under chair C	3	OpSta PLC A28	PLC	PLC OS	Embedded Chair C Controller
104CE1	SERVER FOR CONTROL CONSOLE – LIR ,cabinet V1418	2	Server D A23	Quad CPU Server	Server OS	Driller's Control HMI
104CE2	PLC FOR CONTROL CONSOLE – Drillers cabin, under chair D	3	OpSta PLC A29	PLC	PLC OS	Embedded Chair D Controller

3.9 Software Change Control Process

It is recommended that the Owner and DCO review the Software Change Control Process to determine completeness. Refer to Appendix 7/5

3.11 Software Configuration Management Plan

It is recommended that the Owner and DCO reviews the Software Configuration Management Plan for the following considerations, not inclusive, to determine completeness:

i) Software configuration management activities are planned.

ii) All software work assets are identified, controlled, and available.

iii) All changes to identified software work assets are controlled.

iv) All stakeholders have been informed of the status and content of software baselines.

v) A mechanism is used for controlling changes to the software requirements.

vi) A mechanism is used for controlling changes to the software design.

vii) A mechanism is used for controlling changes to the code.

viii) A mechanism is used for configuration management of the software tools used in the maintenance process.

ix) There is a library of regression tests for maintenance acceptance.

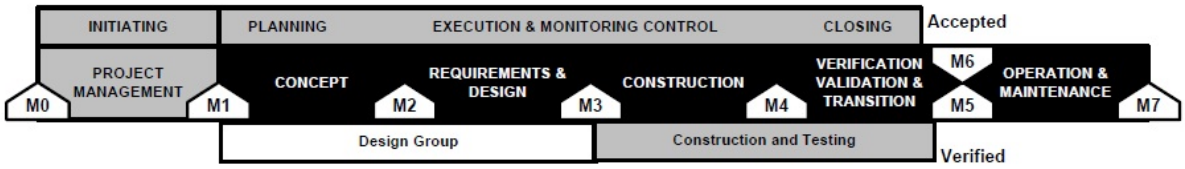
x) The software Configuration Management Plan may be part of the Owner's/DCO's MOC Procedure.

5 Integrated Control System Maintenance

5.1 Scheduled Upgrades – New Functionality

Integrated control system new functionality upgrades are usually the result of replacement of significant computer systems, additions or replacement of major system functionality. Because of the known nature and their significant impact on the unit these upgrades are managed in the same way that the initial system integration occurred. New control system functionality requires that previous SDLC stage gate processes and deliverables be updated. The SDLC effort may be reduced to fit the scope of the project. The difference between a significant and minor upgrade is dependent upon the unit and application of the control system.

FIGURE 1
ISQM SDLC Phase *(1 September 2012)*



5.1.1 Project Management

Develop a project management plan for the scheduled new functionality.

5.1.2 Concept Phase (C) *(1 September 2012)*

If the control system software was developed using a FDD, jump to 8/5.1.4.

i) Review the existing ConOps and update to reflect the new functionality

ii) Define all the new functions.

iii) Safety review of the new functionality.

iv) Review consequences of failure of the function and assign a new Integrity Level with input from other organizations and groups.

v) It is recommended that the verification method for the new functionality is the same as that used for the original verification.

vi) Update all traceability matrices.

5.1.3 Requirements and Design Phase (RD) *(1 September 2012)*

If the control system software was developed using a FDD, jump to 8/5.1.4.

i) Update the existing SRS to reflect the new functionality.

ii) Update the existing SDS to reflect the new requirements.

iii) Update all existing performance, safety, database and security requirements, and adherence to standards, ergonomics consideration, and capabilities.

iv) Define new integration testing for all new commercial off-the-shelf (COTS) packages.

5.1.4 Design Group *(1 September 2012)*

If the control system software was not developed using a FDD, jump to 8/5.1.5.

i) Update the existing FDD to reflect the new functionality.

ii) Update the existing FDD to reflect the new requirements.

iii) Update all existing performance, safety, database and security requirements, and adherence to standards, ergonomics consideration, and capabilities.

iv) Define new integration testing for all new commercial off-the-shelf (COTS) packages.

5.1.5 Construction Phase (CON) *(1 September 2012)*

i) Develop integration code supporting the new functionality.

ii) The SI is to complete all levels of testing as specified in the Construction Phase, refer to Section 5, as per the SRS and SDS or FDD.

5.1.6 Verification, Validation and Transition (V V&T) Phase *(1 September 2012)*

i) Update the Verification Plan (V&V Plan) and configure the simulation for the verification methodology.

ii) Execute the updated V&V Plan.

iii) Transition the integrated system to the Owner and DCO.

iv) Install the software on the target hardware.

v) Functionally test all support services.

vi) Update all documentation and transition back to the O & M stage.

5.3 Unscheduled Upgrades *(1 September 2012)*

Unscheduled upgrades occur when an equipment manufacturer releases hardware, firmware or software upgrades to a control system or a computer hardware manufacturer releases a set of modifications.

For unscheduled upgrades to ISQM control systems or software functions with an Integrity Level IL0 to IL3, the following steps are to be taken:

i) Follow all safety procedures with respect to lock out/tag out.

ii) Follow all the manufacturer's instructions in upgrading the hardware/software.

iii) Using the software and control equipment registries, identify all hardware/software modules that interact with the upgraded hardware/software.

iv) At a minimum, the SI is to peer review of the software code or perform regression tests for all the identified hardware/ software.

v) If all tests pass, prepare to put the upgraded hardware/software into operation.

vi) If any tests failed, contact the manufacturers and return the system to the previous version of hardware/software before the upgrade is attempted.

vii) Update all documentation.

5.3.1

If the upgrade is to a software function that is rated IL2 or IL3, then the process defined in 8/5.1 is to be followed, if time permits, as decided by Owner or DCO.

5.3.2

If not performed prior to the unscheduled upgrade, perform 8/5.1 for IL2 and IL3 ISQM control systems as determined for significant or minor upgrades. At a minimum, the process defined for 8/5.1.2, 8/5.1.3 or 8/5.1.4 is to be followed to update the ConOps, SRS & SDS or the FDD.

5.3.3

For IL0 and IL1 ISQM control systems, it is recommended to follow 8/5.3.i to 8/5.3.vii or, at the Owner's discretion, 8/5.1.

7 System Retirement

Retirement or replacement of the control system is to consider the following in the retirement or replacement plan:

i) During the retirement or replacement activities, control and monitoring is reduced or eliminated. The retirement plan is to consider safeguards for equipment and process during the removal and/or replacement.

ii) No part of the replaced control system is to continue to provide service associated with the control system with the **ISQM** notation listed in the ABS *Record*.

9 O & M Phase, Milestone M7

Retirement of the integrated control system.

SECTION 8

Surveys After Construction and Maintenance of Class

1 General

The provisions of this Section are requirements for the maintenance of classification of the control system(s) associated with the Integrated Software Quality Management (ISQM) notation. These requirements are in addition to the provisions noted in other ABS Rules and/or Guides, as applicable, to the vessel or facility.

For purposes of this Section, the commissioning date will be the date on which a Surveyor issues an Interim Class Certificate to the vessel or facility with the **ISQM** notation.

3 Surveys for the Integrated Software Quality Management Notation

3.1 Survey Intervals and Maintenance Manuals/Records

All Annual and Special Periodical Surveys associated with the **ISQM** notation are to be carried out at the same time and interval as the periodical classification survey of the vessel or facility in order that they are recorded with the same crediting date.

An Annual Survey of the control system(s) associated with the **ISQM** notation is to be carried out by a Surveyor within three months either way of each annual anniversary date of the initial certification survey.

A Special Periodical Survey of the control system(s) associated with the **ISQM** notation is to be carried out within five years of the initial certification survey and at five-year intervals thereafter. ISQM surveys may be offered for survey prior to the due date when so desired, in which case, the survey will be credited as of that date.

Maintenance and calibration records are to be kept and made available for review by the attending Surveyor. The maintenance records will be reviewed to establish the scope and content of the required Annual and Special Periodical Surveys that are to be carried out by a Surveyor. During the service life of the software system components, maintenance records are to be updated on a continuing basis.

3.1.1

The Owner is to inform ABS whenever an IL3 Software Module is modified or installed in the control system with ISQM notation. ABS may audit the vessel upon notification of an IL3 Software Module modification or installation.

3.3 Annual Surveys

At each Annual Survey, the Surveyor is to perform an integrated software and hardware configuration audit to include verification of the following:

i) Change control procedures include periodic audits to confirm that procedures are also being followed.

ii) Examination of Control Equipment Registry per 8/3.3.1

iii) Examination of Software Registry per 8/3.3.2

iv) Review of Integrated Control System's Hardware Registry per 8/3.3.3

v) Review records of virus and malicious software scans.

3.3.1 Examination of Control Equipment Registry

i) Identify control equipment that has been changed since the last audit.

ii) Record each changed equipment item.

iii) List all software hosted on the changed equipment

iv) Identify all documentation impacted by the change

v) Record each documentation change.

vi) Note any changes identified that were not listed on the registry.

3.3.2 Examination of Software Registry

i) Identify all control software that has been changed since the last audit.

ii) Record each software item change.

iii) Inspect all software hosted on the changed equipment identified in step 8/3.3.1.

iv) Record software changes on changed equipment in the Software Registry

v) Identify all documentation impacted by the changes

vi) Record all changed documentation in the software registry

vii) Note any software changes identified that were not listed on the registry

3.3.3 Review of Integrated Control System's Hardware Registry

i) *(1 September 2012)* Assess how closely the software MOC is followed by interviewing relevant Owner/DCO and vendor crew as well as reviewing supporting documentation.

ii) Where possible, identify weaknesses and recommend improvements to the process.

3.5 Special Periodical Surveys

The Special Periodical Survey is to include all items listed under the Annual Survey to the satisfaction of the attending Surveyor.

5 Modifications, Damage and Repairs

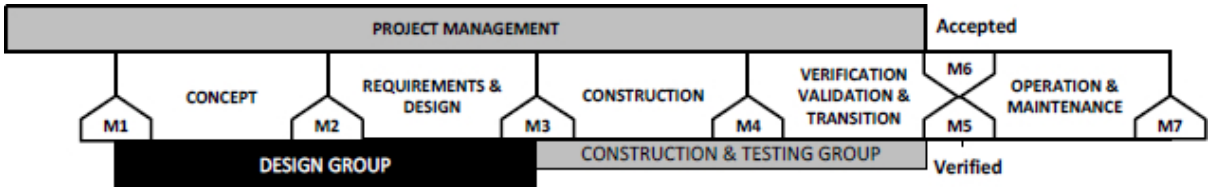
When it is intended to carry out any modifications to the software system that affects the **ISQM** notation of the vessel or facility, the details of such modifications are to be submitted for approval and the work is to be carried out to the satisfaction of the Surveyor.

When a control system that affects the **ISQM** notation of the vessel or facility has suffered any damage, which may affect classification, ABS is to be notified and the damage is to be assessed by a Surveyor.

Where a control system suffers a premature or unexpected failure, and are subsequently repaired or replaced without Surveyor attendance, details of the failure, including the damaged parts where practicable, are to be retained onboard for examination by the Surveyor during the next scheduled survey/ visit. If failures are deemed to be a result of inadequate or inappropriate maintenance, the maintenance manual is to be amended and resubmitted for approval.

SECTION 9

Software Development Life Cycle: Design Group *(1 September 2012)*



1 Scope and Objectives

1.1 General

The goal of the Design Group activities is to produce the Functional Description Documents (FDD). The FDD describes the functions of the equipment controlled by the equipment's control system software with information as listed for the ConOps (Section 3), Software Requirement Specification (SRS) and Software Design Specification (SDS) (Section 4), with exceptions. The FDD replaces the Concept of Operation document (ConOps), Software Requirements Specification (SRS) & the Software Design Specification (SDS) documents in situations where in approximately 85% of the software (software modules or code) is already in use in industry. Risk management, traceability, interface requirements and other FDD content are maintained in a manner consistent with the content of the ConOps, SRS and SDS. The FDD may be a combination of documents and drawings meeting the requirements from this section.

Of particular importance is the Integrity Level assignments to the FDD described functions. The Owner assigns an Integrity Level (IL) to software functions during appropriate stakeholder reviews. Integrity Level assignments are documented in the FDD, which is subsequently referenced for the safety review and FMECA. Specifically, ISQM control system(s) with an overall IL rating of IL1, IL2 or IL3 are subject to safety reviews while ISQM control system(s) with an overall IL rating of IL2 and IL3 systems are subject to software focused functional Failure Mode and Effects Criticality Analysis (FMECA).

Production Software refers to control system software that is approximately 85% reused software modules or code with customization to meet the new or additional requirements or specifications. The SI may alternatively designate the FDD as a Functional Design Specification (FDS), Technical Description Document, Operation Manual, or another similar title.

The SI develops or updates the FDD for review by the Owner, SBI, DCO and ABS. The Owner assigns the Integrity Level (See 3/2) to functions and test scenarios for use in the verification. The SI facilitates a software focused, top down, functional FMECA on IL2 and IL3 control system software.

Please refer to Appendix 9 for a list of activities and submittals for Design Group.

1.3 Requirements for Use of Functional Description Documents

Primary requirements for use of this section to replace the Concept and RD Phase activities are:

i) The control system software to be provided to control or monitor the equipment, control system or integrated system is to be comprised of approximately 85% or more utilizing established functions and code modules or code with the remainder being configuration modifications and/or new code to meet the requirements or specifications.

And

ii) The control system software is to be currently in use within the industry.

a) Multiple updates or modifications that have been made to the control system software over time does not preclude the use of this section and are acceptable to ABS.

Or

iii) The control system software is to be currently in use within the industry.

a) Multiple updates or modifications that have been made to the control system software over time does not preclude the use of this section and are acceptable to ABS.

1.5 Design Group Activities

In the Design Group, the specification for the control system is used to create or update the FDD so that the FDD meets the requirements of Section 9. The FDD contains many attributes of the ConOps in combination with attributes of the SRS and SDS. It is recommended that the processes called out in IEEE 12207 be performed in the development of the new functionality described in the FDD. The recommended steps are:

i) Perform Software Requirements Analysis (4/1.3.1).

ii) Perform Software Architectural Design (4/1.3.2).

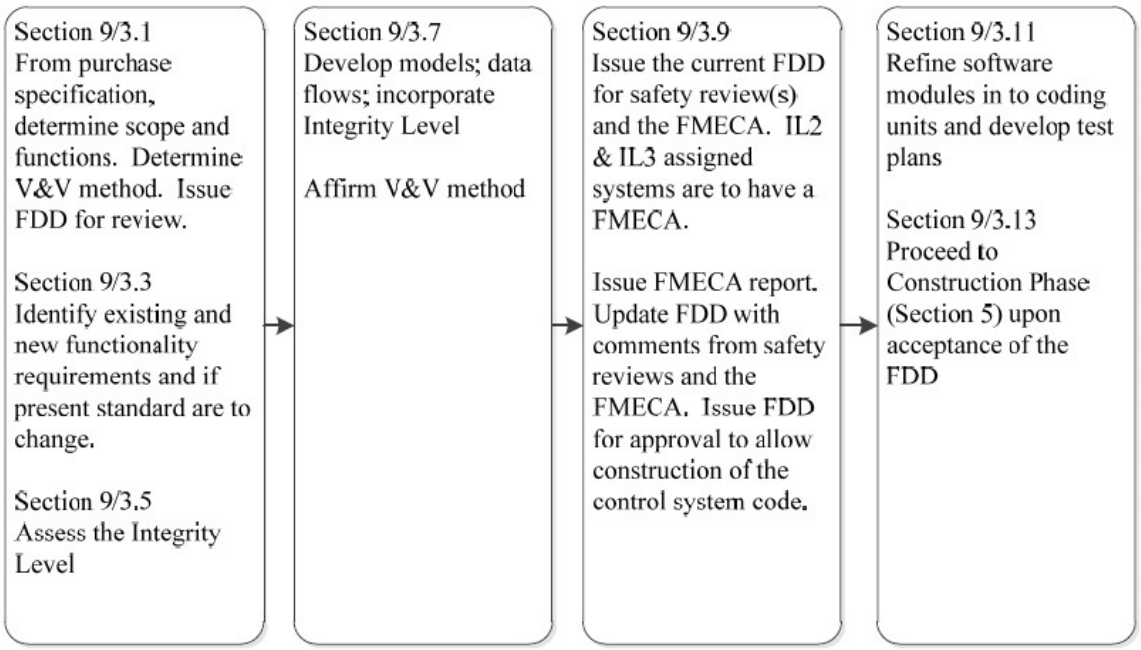
iii) Review criteria and standard for application to new functionality (4/3.1).

iv) Update or create models, as required to facilitate programming (4/3.3).

3 Example Design Phase Process Flow for ISQM

9/3 FIGURE 1 is a nominal depiction of a sequence that could be used to arrive at the Design Group document (FDD) for Production Software.

FIGURE 1
General Flow of Work During the Design Group *(1 September 2012)*



3.1 Scope and Magnitude

The limitations and boundaries of the integrated system are to be defined so as to include any interfaces with hardware and infrastructure components. Traceability of requirements to functionality is introduced.

i) Functions are to be identified and traceable to requirements, designs and safety considerations through all SDLC phases. A Traceability Matrix is recommended. Refer to Appendix A3 for an example Traceability Matrix.

ii) The SI is to state the purpose and scope of the integrated system in the FDD.

iii) The SI is to issue FDD for review.

iv) The Owner with input from the DCO is to review the purpose and scope of the control system.

v) It is recommended that the SI state the verification method for review and consideration by the Owner.

vi) The Owner is to select the verification method (See Section 6).

vii) The software development processes implemented by the SI, the Owner or the SBI are to be mapped to the *ISQM Guide's* SDLC process. (3/1.1.1)

3.3 Identify Existing Functions and New Functions

Detail, modify or create the FDD to include existing, modified or replaced functions and the revised control system. If the standards need to be changed because of new functions, they are to be delineated in the FDD.

3.5 Owner Assigns the Integrity Level

The Owner is to assign the Integrity Level (IL) number to the functions. See 3/2.

3.7 Develop Models

It is recommended that the SI develop integration, data flow and other graphical support documentation, as needed. Refer to Appendix 4 for example models. The Owner's selected verification method is reviewed by the V & V Organization. See 4/3.3.

3.9 Safety Reviews and Failure Mode, Effect and Criticality Analysis

Identification of risk of a software failure and the potential impact to crew safety and the environment is normally performed through safety reviews and FMECA meetings. See 9/5. ABS will not review any business considerations. Please refer to section 3/2.1.1 and 3/2.1.2.

The FDD is issued for review and risk management meetings and analysis. A safety review is to be performed on IL1, IL2 and IL3 ISQM control systems. Safety review reports and FMECA reports are to be submitted for review. Issues uncovered by safety evaluations and FMECA evaluations and the proposed solution(s) are reviewed by the Owner and the SI. Agreed to solutions are then documented in the FDD.

3.11 Identify Coding Units and Test Plans

Decomposition of Software Modules is completed for new, modified or added functions. Internal integration is completed for the new, modified or added functions. Identification of coding units and test plan development are completed. See 4/3.5.

3.13 Proceed to Construction Phase

FDD is updated and issued to Owner, DCO, SBI, and ABS for review. After acceptance from the Owner, proceed to Construction Phase is initiated. See 4/4.

5 Risk Management

Safety reviews and FMECAs are engineering tools that facilitate identification of functions that may impact safety and the environment.

5.1 Integrity Level

The Owner is to assign the Integrity Level (IL) for functions listed in the FDD.

i) The Owner is to refer to Subsection 3/2, 3/7.5 and 3/2.3 TABLE 3 for a description of the IL assignment and development and traceability of requirements.

5.3 Safety Reviews and FMECA

i) A safety review is to be performed on ISQM control systems to which IL1, IL2 and IL3 designations are assigned.

- The safety review may be combined with other safety or operability reviews, hardware FMEA, or evaluations, or software FMECA.
- It is recommended that SI, Owner, DCO, IA, SBI and ABS be present during the safety reviews.

ii) A FMECA is to be performed on ISQM control systems to which IL2 and IL3 designations are assigned. See 4/5.5.4 and 4/5.5.5.

5.5 New or Unproven Technology

Refer to 3/5.1.4 for new or unproven technology.

7 Functional Description Document (FDD)

The FDD contains attributes and content of the ConOps, SRS & SDS documents, with exceptions. The SI is to have the discretion to include or not include software functional proprietary information or intellectual property of the SI in the FDD. The SI is to describe the functions in descriptive terms.

7.1 Requirements of the ISQM System Integrator's FDD

7.1.1

General description of the scope and purpose of the control system or an introduction.

7.1.2

Fail safe states of the equipment under control [3/2.2, 3/7.1.iii.c].

i) When the function is controlled and performed by another supplier's equipment, state to refer to the supplier's documentation.

7.1.3

The FDD is to describe the functions of the ISQM control system:

i) Each function is to have an identifier for traceability [4/5.9.1.i].

ii) Each function characterized by new or unproven technology is to be so identified (4/5.5.5).

iii) Each function associated with a Safety Instrumented System is to be so identified [4/5.9.1.iv].

iv) Each function associated with an essential system is to be so identified [4/5.9.1.iv].

v) Each function is to have the normal, degraded and failed conditions (states) of the control system functions, as follows [3/2.2, 3/7.1.iii.c, 4/5.9.1.ii]:

- ***a)*** Normal state of the function for IL0 to IL3 functions.
- ***b)*** Failed state(s) of the function for IL1 to IL3 functions
- ***c)*** Degraded state(s) of the function for IL2 and IL3 functions.

Note:

The SI may use the FMECA format for the presentation of the functions in preparation for the FMECA that is to follow the FDD.

7.1.4

i) When the function is controlled and performed by another supplier's equipment, the FDD is to identify the supplier, state the nature of that external control and refer to the supplier's documentation concerning the external control.

ii) The FDD is to describe the interface and communication protocol of functions as required for the connected equipment [3/7.1.vi, 4/5.9.1.vi, 4/5.9.1.viii, 4/5.9.1.vi]. This may also be a topology drawing with communication protocols listed.

7.1.5

Number and description of interfaces for Human Machine Interfaces (HMI) is to include [3/7.1.iv]:

i) Quantity of HMI network or direct connections to the ISQM control system

ii) Manufacturer or the SI's or Supplier's part number

iii) Model number or the SI's or Supplier's part number

iv) Firmware and software version, if known at this time.

v) Interface protocol

vi) Constraints

7.1.6

Number and description of interfaces (non HMI and include: SCADA, data collection, etc.) is to include [3/7.1.v), 4/5.9.1.viii]:

i) Quantity of network or direct connections to the ISQM control system

ii) Interface protocol of interfaced network, control system and/or equipment

iii) Constraints of interfaced network, control system and/or equipment

7.1.7

The FDD is to include descriptions of any unresolved functional system conflicts.

7.1.8

The FDD is to include high-level descriptions of the control systems Obsolescence Plans:

i) Hardware Obsolescence plan (3/5.9.1)

ii) Software Obsolescence plan (3/5.9.2)

7.1.9

Safety review and FMECA reports are to be submitted separately from FDD.

7.3 Requirements of the ISQM SI's Control System Supplier's Section of the FDD

The other sections of the FDD are to include the supplier's information, and other pertinent information.

i) System specification:

a) System Specification is to be updated at the end of the Construction Phase, as appropriate.

7.3.1

System Integrators or software Suppliers information is to be attached to the FDD:

i) The SI is to place the supplier's information within the FDD section.

ii) Description of the equipment functions. This could also be the Supplier's FDD.

iii) Process Conditions are to be defined [4/5.9.1.viii]:

a) Design Limits

b) Operating Limits

c) Alarm points

iv) Interface Requirements are to be specified [4/5.9.1.viii].

v) Interface registers are listed:

a) The purpose of the interface registers is defined.

vi) Supplier's equipment is assigned an IL2 or IL3 by the Owner, the Supplier develops and deliver the Verification Plan (V & V Plan) for equipment interfaced with the SI's control system.

a) It is permissible for the V & V Plan to be delivered during the Construction Phase.

vii) Supplier's equipment is assigned an IL1, IL2 or IL3 by the Owner, the Supplier is to provide the Verification Report (V & V Report) for the equipment interfaced with the SI's control system:

a) It is permissible for the V & V Report to be delivered during the Construction Phase.

b) If the supplier's control system function has been assigned IL2 or IL3, ABS and the IA are to witness the verification.

c) If the supplier's control system functions have been assigned IL1 designations, ABS may witness the verification at the Owner's option. The IA may witness the verification of IL0, IL1, IL2 and IL3 designated control systems.

9 V & V activities during the Design Group

i) The V&V Organization is to develop a high-level initial draft of the ISQM SI's V & V Plan.

ii) The ISQM SI's V&V Plan is to be reviewed by:

a) ABS and the Independent Auditor

b) It is recommended that the Owner and DCO review the V & V Plan.

11 Deliverables

The ISQM SI's FDD is to be provided to the Owner or SBI.

13 Milestones

13.1 Design Group Complete, Milestone M3

The M3 Milestone signifies that:

i) The FDD has been updated with safety review(s) and FMECA (for IL2 and IL3 control systems), etc. including any remediation recommendations that have been accepted.

ii) Integrity Levels are assigned to FDD functions.

iii) The primary ISQM control system's V & V method has been selected.

iv) FDD has been reviewed by Owner, DCO, SBI, IA, and ABS. Review period as per contract or other agreement with the contracting party.

13.3 Authorization from the Owner to Proceed to the Construction Phase

The Owner and ABS, with input from the IA, are to approve the FDD to proceed to the Construction Phase. Review period as per contract or other agreement with the contracting party.

APPENDIX 1

Activities and Requirements of Organizations *(1 September 2012)*

To promote clarity, the following tables show activities of each organization during the execution of all phases. The abbreviations are from the following table:

Phase – Organization – Tracking Number

PHASE	*ORGANIZATION*
C = Concept	OW = Owner (Note 1)
R&D = Requirements & Design	DCO = Driller or Crew
	SI = System Integrator
CON = Construction	IA = Independent Auditor
V V&T = Verification, Validation & Transition	V&V = Verification & Validation
OM = Operate & Maintenance	CT = Subcontractor

Example: The Owner in the Concept Phase has a requirement, deliverable or activity number #1 then this activity is "C-OW-R1". The System Integrator has an activity # 5 in the Concept Phase, then this activity is "C-SI-A5"

The documents and data requested by ABS in Appendix A1 tables are used to support ABS's reviews of the required submittals.

In the following tables, Y = Yes and N = NO.

Note:

1 The Owner is the organization which provides funding and initiates the project. The Shipyard or Builder may be the Owner during the construction of the vessel or offshore unit.

1 Concept Phase Activities

1.1 Concept Phase Owner's (OW) Activities

Tracking Number	*Concept Phase Owner's (OW) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-OW-A1	Assign roles and responsibilities, Owner's team members, DCO, System Integrator		0, 1, 2, 3	---	N	N	N	N
C-OW-A2	Assign Owner's team members	Owner sets up the team.	0, 1, 2, 3	---	N	N	N	N
C-OW-R3	Update overall project and Generic System requirements	Owner leads and participates in mission statement, objectives of the overall project. Part of ConOps	0, 1, 2, 3	3/1.1.1 & 3/7.3	Y	Y	Y	Y
C-OW-R4	Develop MOC procedure for the integrated control system		0, 1, 2, 3	3/1.1.1	Y	Y	Y	Y
C-OW-A5	Development process are to be traced to Guide's SDLC		0, 1, 2, 3	3/1.1.1	Y	Y	Y	Y
C-OW-A6	Design tradeoffs, conflicts resolved	Part of ConOps	0, 1, 2, 3	3/1.1.1	N	N	N	N
C-OW-A7	Identify integrated system components	Part of ConOps	0, 1, 2, 3	3/1.1.1	N	N	N	N
C-OW-A8	ARMS consideration	Part of ConOps	0, 1, 2, 3	3/5.9.1 & 3/4.1	N	N	N	N
C-OW-A9	Lead or manage safety review(s), provide resultant documentation	Owner may facilitate or have a third party facilitate the safety review(s). Owner is to involve DCO, IA and SI at a minimum.	0, 1, 2, 3	3/4.1	Y	Y	Y	Y
C-OW-A10	Provide integrity level definition used	Part of ConOps	0, 1, 2, 3	3/5.3.5	Y	Y	Y	Y

Tracking Number	*Concept Phase Owner's (OW) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-OW-R11	Essential systems are to have another means of operation independent from the Integrated System	ABS *Marine Vessel Rules* 4-9-2/13.13. Interconnection between ISQM control system and local control is to be delineated in the ConOps. Part of ConOps	2, 3	---	N	N	N	N
C-OW-A12	Assign IL number to all functions of the ISQM control system	Part of ConOps	0, 1, 2, 3	3/4.1	N	N	N	N
C-OW-A13	Select verification method	Refer to Section 8.Part of ConOps	0, 1, 2, 3	3/7.1	N	N	N	N
C-OW-A14	Incorporate Suppliers V&V Reports & /or V&V Plans for packages	V&V Report for IL1, 2, 3 and V&V Plan for IL2, 3. Part of ConOps	0, 1, 2, 3	3/7.7.2, 3/7.7.3 & 3/4.1	N	N	N	N
C-OW-R15	Develop and provide ConOps for review	Refer to 3/7, 3/4 and Appendix 3 for additional details	0, 1, 2, 3	3/7 & 3/4	Y	Y	Y	Y
C-OW-R16	Report of consolidated comments of the ConOps review	Provide to DCO and SI. Consolidate report to ABS	0, 1, 2, 3	3/5.1.3 & 3/4.1	Y	Y	Y	Y
C-OW-A17	Recommended metrics	See Appendix 8	0, 1, 2, 3	A8/23	N	N	N	N
C-OW-A18	Supply supportive information to the System Integrator, involved in the Concept Phase, if any	Owner provides the supportive information to the System Integrator	0, 1, 2, 3	---	N	N	N	N
C-OW-A19	Choose lifecycle management of the integrated system	Based on the type of integrated system, the proper lifecycle management is selected with input from the SI	0, 1, 2, 3	3/4.1	N	N	N	N
C-OW-R20	Grant Authorization to proceed to the RD Phase	Approve the ConOps	0, 1, 2, 3	3/11.3	N	N	N	N

1.3 Concept Phase Driller or Crew's (DCO) Activities

Tracking Number	*Concept Phase Driller or Crew's (DCO) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-DCO-A1	Assign DCO's team members	DCO sets up the team.	0, 1, 2, 3	---	N	N	N	N
C-DCO-A2	Assign roles and responsibilities to DCO's team members	DCO is to assign the roles and responsibilities to its team members.	0, 1, 2, 3	---	N	N	N	N
C-DCO-A3	Assist Owner with tradeoffs, conflict resolution	Part of ConOps	0, 1, 2, 3	---	N	N	N	N
C-DCO-A4	Assist with establishing minimum requirements and design		0, 1, 2, 3	---	N	N	N	N
C-DCO-A5	Participate in safety review(s)		0, 1, 2, 3	3/5.1.3	N	N	N	N
C-DCO-A6	Participate in Integrity Level assignment meeting, if requested		0, 1, 2, 3	3/2.2	N	N	N	N
C-DCO-A7	Support Owner and System Integrator with information requests		0, 1, 2, 3	---	N	N	Y	N
C-DCO-R8	ConOps Review	Provide to OW for consolidated report	0, 1, 2, 3	3/5.1.3	N	N	N	N
C-DCO-A9	Provide additional detail for 1) integrated system's components description, 2) Descriptions of functions action during normal, degraded or failed condition	Part of ConOps IL0 functions have only normal condition described.	0, 1, 2, 3	---	N	N	N	N

1.5 Concept Phase System Integrator's (SI) Activities

Tracking Number	*Concept Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-SI-A1	Collect Owner's requirements		0, 1, 2, 3	---	N	N	N	N
C-SI-A2	Assign Integrator's senior technical member(s)		0, 1, 2, 3	---	N	N	N	N

Tracking Number	*Concept Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-SI-R3	Provide current ISO9001 or CMMI Level 2 certificate	Provide to OW and ABS	0, 1, 2, 3	2/3.1.2	Y	N	Y	N
C-SI-A4	Development process are to be traced to Guide's SDLC	Part of ConOps	0, 1, 2, 3	3/1.1.1	N	N	N	N
C-SI-A5	Collect subcontractors constraints		0, 1, 2, 3	3/1.1.1	N	N	N	N
C-SI-A6	Design tradeoffs, conflict resolution	Part of ConOps	0, 1, 2, 3	3/1.1.1	N	N	N	N
C-SI-R7	If a Canonical Integration Model was developed, then provide to organizations		0, 1, 2, 3	3/1.1.1.i	Y	Y	Y	Y
C-SI-A8	Assist Owner with identifying all Integrated System functions	Essential functions are IL2 or IL3. SIS are to be IL3 assigned.	0, 1, 2, 3	3/2.1.1 & 3/5.1.4	N	N	N	N
C-SI-R9	Identify new or novel essential functions or SIS functions in the integrated system	Essential functions are IL2 or IL3. SIS are IL3. Part of ConOps	2, 3	3/5.1.4	N	N	N	N
C-SI-A10	System Requirement Analysis	Part of ConOps	0, 1, 2, 3	3/1.1.2	N	N	N	N
C-SI-A11	Attend safety review meetings		0, 1, 2, 3	3/2.1.2	N	N	N	N
C-SI-A12	Assist the Owner with IL assignment	Essential functions are IL2 or IL3. SIS are IL3. Part of ConOps	0, 1, 2, 3	3/2	N	N	N	N
C-SI-A13	System Integration Architectural Design	Part of ConOps	0, 1, 2, 3	3/1.1.3	N	N	N	N
C-SI-A14	Obsolescence plan for hardware	Define obsolescence strategy for hardware and provide to OW. Part of ConOps	0, 1, 2, 3	3/5.9.1	N	N	N	N
C-SI-A15	Obsolescence plan for software	Define obsolescence strategy for software and provide to OW. Part of ConOps	0, 1, 2, 3	3/5.9.2	N	N	N	N

Tracking Number	*Concept Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-SI-A16	Review Verification method selected	Comment on feasibility	0, 1, 2, 3	---	N	N	N	N
C-SI-R17	Review ConOps	Provide to OW for consolidated report	0, 1, 2, 3	3/5.1.3	N	N	N	N

1.7 Concept Phase Subcontractors'(CT) Activities

Tracking Number	*Concept Phase Subcontractor's (CT) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-CT-A1	Deleted							
C-CT-A2	Provide equipment limitation or constraints to requesting organization		0, 1, 2, 3	---	N	N	N	N
C-CT-A3	V & V Report for packages that are to be provided that are connected to the ISQM control system	IL1, IL2 & IL3 packages or functions Part of ConOps	1, 2, 3	3/7.7.2	N	N	N	N
C-CT-A4	V & V Plan for packages that are to be connected to the ISQM control system	IL2 & IL3 packages or functions Part of ConOps	2, 3	3/7.7.3	N	N	N	N
C-CT-R5	Current ISO 9001 certificate		0, 1, 2, 3	2/3.1.7	Y	N	Y	N
C-CT-A6	Review canonical integration model. Use canonical model in design	Send comments to the SI	0, 1, 2, 3	3/1.1.1.i	N	N	N	N

1.9 Concept Phase Verification & Validation (V & V) Activities

Tracking Number	*Concept Phase Verification & Validation's (V & V) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
C-VV-A1	Deleted							
C-VV-A2	Provide schedule to requesting organization	V & V is to provide schedule to organization who requests	0, 1, 2, 3	---	N	N	N	N
C-VV-A3	Review canonical integration model from SI	Send comments to the SI	0, 1, 2, 3	3/1.1.1.i	N	N	N	N

1.11 Concept Phase Independent Auditor's (IA) Activities

Tracking Number	*Concept Phase Independent Auditor's (IA) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*
C-IA-A1	Participate in safety review(s)		0, 1, 2, 3	3/2.1.2	N	N
C-IA-A2	Participate in IL Assessment meeting	Comment on following OW rules for IL assignments	0, 1, 2, 3	---	N	N
C-IA-A3	ConOps Review	Send comments to the Owner	0, 1, 2, 3	3/7	N	N
C-IA-A4	Review V & V method selected by Owner.	Provide comments to OW, SI Part of ConOps	0, 1, 2, 3	3/4.1	N	N

3 Requirements and Design (RD) Phase Activities

3.1 RD Phase Owner's (OW) Activities

Tracking Number	*RD Phase Owner's (OW) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
RD-OW-A1	Update ConOps following the MOC. Provide ABS with SRS & SDS	During SRS & SDS development, changes may be required in the ConOps	0, 1, 2, 3	4/5.5.6	Y	Y	Y	Y
RD-OW-R2	SRS and SDS review and approval	For consistency with the ConOps document approval or provide comments	0, 1, 2, 3	4/1.2.1	N	N	N	N
RD-OW-A3	Participate in FMECA	Project and operational risks	2, 3	4/5.5	N	N	N	N
RD-OW-R4	Safety review for any added functions or supplier's packages	Update ConOps	0, 1, 2, 3	4/5.5.6	Y	Y	Y	Y
RD-OW-R5	Grant Authorization to proceed to the Construction Phase		0, 1, 2, 3	4/11.vi	Y	N	Y	N

3.3 RD Phase Driller or Crew's (DCO) Activities

Tracking Number	*RD Phase Operator's (OP) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
RD-DCO-A1	SRS and SDS Review	For consistency with the ConOps Comments to SI	0, 1, 2, 3	4/1.2.1	N	N	N	N
RD-DCO-A2	Support Owners and SI activities		0, 1, 2, 3	---	N	N	N	N

3.5 RD Phase System Integrator's (SI) Activities

Tracking Number	*RD Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
RD-SI-A1	SI to assign integration team members		0, 1, 2, 3	---	N	N	N	N
RD-SI-A2	Deleted							
RD-SI-A3	Update canonical integration model, if developed, pass to Suppliers		0, 1, 2, 3	---	Y	Y	Y	Y
RD-SI-A4	Functions are to be refined and detailed in the SRS		0, 1, 2, 3	4/1.2.1	N	N	N	N
RD-SI-A5	Functions are to be refined and detailed in the SDS		0, 1, 2, 3	4/1.3.4	N	N	N	N
RD-SI-A6	From the ConOps, add V & V scenarios for operational and non-operational states		1, 2, 3	4/5.9	N	N	N	N
RD-SI-A7	The functions within are to be traceable to ConOps and safety review(s)	Functions are to be traceable from ConOps to SRS and SDS	1, 2, 3	4/1.3.2(a)	N	N	N	N
RD-SI-A8	V & V Plan and/or V & V Report for Supplier's packages	If not provided previously for ConOps. Suppliers to provide to SI, issue to the Owner and ABS	0, 1, 2, 3	3/7.7.2 & 3/7.7.3	Y	Y	Y	Y
RD-SI-A9	SI to facilitate and participate in Software Control System FMECA meetings		2, 3	4/5.5.4	N	N	N	N

Tracking Number	*RD Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
RD-SI-A10	Provide Software Control System FMECA report(s)		2, 3	4/5.5.2, 4/5.5.3 & 4/5.5.4	Y	Y	Y	Y
RD-SI-A11	SI to update and approve the SRS and SDS per the functional FMECA and comments from reviews	OW to update the ConOps	2, 3	4/5.5.4	N	N	N	N
RD-SI-A12	Supplier's package documentation	To be considered in the overall plan	0, 1, 2, 3	4/5.5.3	N	N	N	N
RD-SI-R13	Variance from standards report(s)		0, 1, 2, 3	4/9	Y	Y	Y	Y
RD-SI-R14	Publish SRS		0, 1, 2, 3	4/4	Y	Y	Y	Y
RD-SI-R15	Publish SDS		0, 1, 2, 3	4/4	Y	Y	Y	Y
RD-SI-R16	Provide consolidated SRS and SDS review report		0, 1, 2, 3	4/5.7	Y	Y	Y	Y

3.7 RD Phase Subcontractors'(CT) Activities

Tracking Number	*RD Phase Subcontractor's (CT) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
RD-CT-A1	Support the SI activities		0, 1, 2, 3	---	N	N	N	N
RD-CT-R2	If not previously provided, current ISO 9001 certificate.		0, 1, 2, 3	2/3.1.7	N	N	N	N
RD-CT-R3	Participate in the software FMECA	SI is to organize FMECA		---	N	N	N	N

3.9 RD Phase Verification & Validation (V&V) Activities

Tracking Number	*RD Phase Verification & Validation (V & V) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
RD-V&V-R1	Draft initial V&V plan	Occurs towards the end of the RD Phase. Provide to SI, OW & OP	0, 1, 2, 3	4/7	Y	Y	Y	Y

3.11 RD Phase Independent Auditor's (IA) Activities

Tracking Number	*RD Phase Independent Auditor's (IA) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*
RD-IA-A1	Perform independent selected design reviews	Provide reports to ABS	0, 1, 2, 3	---	Y	Y
RD-IA-R2	SRS and SDS Review	Review for consistency with the ConOps. Review V & V requirements for IL2 & IL3 functions	0, 1, 2, 3	4/1.2.1	N	N

5 Construction (CON) Phase Activities

5.1 Construction Phase Owner's (OW) Activities

Tracking Number	*Construction Phase Owner's (OW) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-OW-R1	Manage change requests per MOC policy	Update ConOps as required per MOC. Refer to CON-OW-R9	0, 1, 2, 3	---	N	N	N	N
CON-OW-A2	Track Risks	Project and operational	0, 1, 2, 3	---	N	N	N	N
CON-OW-A3	Monitor project progress against plan		0, 1, 2, 3	---	N	N	N	N
CON-OW-A4	Support SI activities		0, 1, 2, 3	---	N	N	N	N
CON-OW-A5	Review results of SI's overall test results	Integration test results	0, 1, 2, 3	5/1.iv	Y	Y	Y	Y
CON-OW-R7	Review and approve updates to SRS and SDS or FDD		0, 1, 2, 3	5/5.5	Y	Y	Y	Y
CON-OW-R8	Review ConOps per updates to SRS and SDS or FDD		0, 1, 2, 3	5/5.5	Y	Y	Y	Y
CON-OW-R9	Reissue ConOps when programming is 90% complete.	ConOps is to be updated with all known information prior to issuance. Used in the V V&T Phase to begin validation activities	0, 1, 2, 3	6/4	Y	Y	Y	Y
CON-OW-R10	Review the V&V Plan		0, 1, 2, 3	5/7.1	N	N	N	N

5.3 Construction Phase Driller or Crew's (DCO) Activities

Tracking Number	*Construction Phase Driller or Crew's (DCO) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-DCO-A1	Manage change requests per MOC		0, 1, 2, 3	---	N	N	N	N
CON-DCO-A2	Support SI activities		0, 1, 2, 3	---	N	N	N	N
CON-DCO-A3	Review results of SI overall test results		0, 1, 2, 3	5/1.iv	N	N	N	N
CON-DCO-A4	Review updates to the ConOps		0, 1, 2, 3	5/5.5	N	N	N	N
CON-DCO-A5	Review updates to SRS and SDS		0, 1, 2, 3	5/5.5	N	N	N	N
CON-DCO-A6	Review the V&V Plan		0, 1, 2, 3	5/7.1	N	N	N	N

5.5 Construction Phase System Integrator's (SI) Activities

Tracking Number	*Construction Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-SI-A1	Monitor for issues between stakeholders, Suppliers and subcontractors	Resolve Issues	0, 1, 2, 3	---	N	N	N	N
CON-SI-A2	Issue contracts to subcontractors	If not already done and as appropriate	0, 1, 2, 3	---	N	N	N	N
CON-SI-A3	Monitor subcontractors	The SI is to have enough visibility and communications with Suppliers that they are following the canonical integration model.	0, 1, 2, 3	---	N	N	N	N
CON-SI-R4	Peer reviews of coding		2, 3	5/1.1.1(a)	N	N	N	N
CON-SI-A5	Management of Construction activities		1, 2, 3	6/1	N	N	N	N
CON-SI-A6	Review or initiate MOCs (change requests)	As needed	0, 1, 2, 3	---	N	N	N	N
CON-SI-R7	Provide consolidated test results for review	SI's internal testing of modules and overall system	0, 1, 2, 3	5/1.iv	Y	Y	Y	Y

Tracking Number	*Construction Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-SI-A8	Forecast to complete reports	to be provided to the Owner	0, 1, 2, 3	---	N	N	N	N
CON-SI-A9	Deliverable summation reports noting any open issues		0, 1, 2, 3	---	Y	Y	Y	Y
CON-SI-R10	Provide updated or current SRS and SDS or FDD	When construction of the integrated software is 90% complete	0, 1, 2, 3	6/4	Y	Y	Y	Y
CON-SI-A11	Issue Schedule updates as requested by Owner	Recommended from at least monthly	0, 1, 2, 3	---	N	N	N	N
CON-SI-A12	Review the V&V Plan		0, 1, 2, 3	5/7.1	N	N	N	N
CON-SI-R13	Report any variance to standard	As needed	0, 1, 2, 3	4/4	Y	Y	Y	Y

5.7 Construction Phase Subcontractors'(CT) Activities

Tracking Number	*Construction Phase Subcontractor's (CT) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-CT-R1	Review or initiate MOCs (change requests)		0, 1, 2, 3	---	N	N	N	N
CON-CT-A2	Develop and deliver contracted package equipment and associated software		0, 1, 2, 3	---	N	N	N	N
CON-CT-A3	Develop or provide required documentation		0, 1, 2, 3	---	N	N	N	N

5.9 Construction Phase Verification & Validation (V&V) Activities

Tracking Number	*Construction Phase Verification & Validation (V & V) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-V & V-R1	Monitor and incorporate approved SRS and SDS or FDD changes	In the V & V Plan	0, 1, 2, 3	---	N	N	N	N
CON-V & V-A2	Develop V & V Plan	Following SRS and SDS or FDD	0, 1, 2, 3	6/3	Y	Y	Y	Y

Tracking Number	*Construction Phase Verification & Validation (V & V) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
CON-V & V-R3	Issue V & V Plan for review and after review, issue for construction		0, 1, 2, 3	5/7.1	Y	Y	Y	Y
CON-V & V-A4	V & V's PM to monitor V & V configuration against plan		0, 1, 2, 3	---	N	N	N	N
CON-V & V-A5	Develop simulation software	Configure the simulator	0, 1, 2, 3	6/3	N	N	N	N
CON-V & V-A6	Peer Review the simulator software or configuration	Peer review is internal to the V & V Organization	0, 1, 2, 3	6/3	N	N	N	N
CON-V & V-R7	Generate a consolidated report from all V & V Plan comments		0, 1, 2, 3	5/7.1	Y	Y	Y	Y
CON-V & V-R8	Validate the simulation	Peer reviews	1, 2, 3	6/3	Y	Y	Y	Y

5.11 Construction Phase Independent Auditor's (IA) Activities

Tracking Number	*Construction Phase Independent Auditor's (IA) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*
CON-IA-A1	Review V & V Plan	Compare against the SRS, SDS and ConOps	0, 1, 2, 3	5/7.1	N	N
CON-IA-A2	Monitor SI and subcontractors for compliance with the Guide.		1, 2, 3	---	N	N
CON-IA-A3	Perform independent selected design reviews	Provide report to ABS	0, 1, 2, 3	5/1.v	Y	Y
CON-IA-A4	Review ConOps, SRS and SDS or FDD		0, 1, 2, 3	5/5.5	N	N

7 Verification, Validation and Transition (V V&T) Phase Activities

7.1 Verification & Validation Phase Owner's (OW) Activities

Tracking Number	*Verification, Validation & Transition Phase Owner's (OW) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-OW-A1	It is recommended that the OW participate in the V & V verification activities.	Watch for concept errors. Update ConOps as necessary, may require safety reviews of new functionality	1, 2, 3	7/1	N	N	N	N
V V&T-OW-A2	Transfer to DCO the change management after the Acceptance Stage Gate	DCO to manage software changes per the MOC procedure	0, 1, 2, 3	---	N	N	N	N
V V&T-OW-R3	When a Moderate Defect is detected on an IL2 assigned functions, a safety review is to be performed on the proposed workaround. Workarounds are not permitted for IL3 assigned functions.	SI to organize and facilitate the safety review	1, 2	6/7.1 TABLE 2	N	N	N	N
V V&T-OW-A4	Review and approve defects ranking.		0, 1, 2, 3	7/4	N	N	N	N
V V&T-OW-R5	Review V & V Report		0, 1, 2, 3	6/1.1	N	N	N	N
V V&T-OW-A6	Review and approve the V&V Plan	Input from DCO & SI	0, 1, 2, 3	6/9.3	N	N	N	N

7.3 Verification & Validation Phase Driller or Crew's (DCO) Activities

Tracking Number	***Verification, Validation & Transition Phase Driller or Crew's (DCO) Activities***	***NOTES***	***IL Tracking Number***	***Ref***	***Provide to ABS***	***ABS Review***	***Provide to IA***	***IA Review***
V V&T-DCO-A1	It is recommended that the DCO participate in the V&V verification activities.	Watch for concept errors	0, 1, 2, 3	7/1	N	N	N	N
V V&T-DCO-R2	Review V&V Plan		0, 1, 2, 3	6/9.3	N	N	N	N

Tracking Number	*Verification, Validation & Transition Phase Driller or Crew's (DCO) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-DCO-R3	Review V&V Report	Provide comments to Owner	0, 1, 2, 3	6/1.1	N	N	N	N
V V&T-DCO-A4	Provide input for defect ranking by V&V organization.		0, 1, 2, 3	7/4	N	N	N	N

7.5 Verification & Validation Phase System Integrator's (SI) Activities

Tracking Number	*Verification, Validation & Transition Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-SI-A1	Participate in the V&V verification activities.		1, 2, 3	---	N	N	N	N
V V&T-SI-R2	Software is 'locked' after it has passed the verification test		0, 1, 2, 3	7/1	N	N	N	N
V V&T-SI-R3	When a Moderate Defect is detected on an IL2 assigned functions, a safety review is to be performed on the proposed workaround. Workarounds are not permitted for IL3 assigned functions.	SI is to facilitate and participate in the safety review. SI to develop and provide report on the safety review(s)	1, 2	7/4	Y	Y	Y	Y
V V&T-SI-R4	Correct coding defects		0, 1, 2, 3	6/1.1	N	N	N	N
V V&T-SI-A5	Provide input to rank defects by V&V organization.		0, 1, 2, 3	7/4	N	N	N	N

7.7 Verification & Validation Phase Subcontractors'(CT) Activities

Tracking Number	*Verification, Validation & Transition Phase Subcontractor's (CT) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-CT-A1	Provide requested information to support anomaly identification		0, 1, 2, 3	---	N	N	N	N

7.9 Verification & Validation Phase Verification & Validation (V&V) Activities

Tracking Number	*Verification, Validation & Transition Phase Verification & Validation (V&V) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-V&V-R1	Peer review simulation configuration. Produce a simulation configuration report after peer review		0, 1, 2, 3	6/1.5.1	Y	Y	Y	Y
V V&T-V&V-A2	Provide V & V Plan for comment & provide approved V & V Plan		0, 1, 2, 3	6/9.3	Y	Y	Y	Y
V V&T-V&V-A3	Execute the V & V Plan	Perform verification from a black box perspective	1, 2, 3	---	N	N	N	N
V V&T-V&V-A4	Note any deviations from the V & V Plan	Place deviations in the V & V Report(s)	0, 1, 2, 3	7/6	Y	Y	Y	Y
V V&T-V&V-R5	Produce a V & V Report of all anomalies discovered and consolidate comments from other reviewers	Reviewed by OW, DCO, IA and ABS	0, 1, 2, 3	6/11.1	Y	Y	Y	Y
V V&T-V&V-R6	Results of the virus scan.	To proceed, all virus or other malicious software is to be removed.	0, 1, 2, 3	7/1.1	Y	Y	Y	Y
V V&T-V&V-R7	The simulator is to include connected components data (monitoring and control) commands to and from the integrated system, signals, software interlocks and alarms, as necessary.	To verify the integrated system's code and clearly demonstrate the control system software to the stakeholders as specified in the SRS and SDS or FDD.	0, 1, 2, 3	7/3	N	N	N	N
V V&T-V&V-R8	Generate interim V & V Report(s)	As required. Issue to OW, DCO, IA, SI and ABS	0, 1, 2, 3	6/11.1	Y	Y	Y	Y

Tracking Number	*Verification, Validation & Transition Phase Verification & Validation (V&V) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-V&V-R9	Support safety reviews of proposed Moderate Defects work around for IL2 assigned functions	SI to facilitate safety reviews of IL2 workarounds. Workarounds are not permitted for IL3 assigned functions.	1, 2	6/7.1 TABLE 2	N	N	N	N
V V&T-V&V-A10	Rank defects	OW and DCO to approve ranking. Other input from SI, IA organizations and ABS.	0, 1, 2, 3	6/7.1 TABLE 2	Y	Y	Y	Y

7.11 Verification & Validation Phase Independent Auditor's (IA) Activities

Tracking Number	*Verification, Validation & Transition Phase Independent Auditor's (IA) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
V V&T-IA-A1	Review V&V Plan		0, 1, 2, 3	6/9.3	N	N	N	N
V V&T-IA-A2	Monitor V&V organization's team in executing the V&V Plan.	Watch for concept errors. ABS is to witness testing of IL1, IL2, & IL3 systems	0, 1, 2, 3	---	N	N	N	N
V V&T-IA-R3	Review interim V&V Report		1, 2, 3	6/11.1	N	N	N	N
V V&T-IA-R4	Final V&V Report reports		0, 1, 2, 3	6/11.1	N	N	N	N
V V&T-IA-R5	Review results of the virus scan	To proceed, all viruses or other malicious Integrated System software is to be removed.	0, 1, 2, 3	7/1.1	N	N	N	N
V V&T-IA-A6	Provide input to the ranking of defects		0, 1, 2, 3	7/4	N	N	N	N
V V&T-IA-R7	Witness the Verification	Optional witnessing for IL0 and IL1	2, 3	---	N	N	N	N

9 Operation and Maintenance (O & M) Phase Activities

9.1 Operation and Maintenance Phase Owner's (OW) Activities

Tracking Number	*Operation and Maintenance Phase Owner's (OW) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
OM-OW-A1	Develop and manage MOC procedure. Manage MOC requests		0, 1, 2, 3	---	N	N	N	N
OM-OW-A2	Monitor obsolescence	Hardware & Software	0, 1, 2, 3	---	N	N	N	N
OM-OW-R3	Review O & M plan		0, 1, 2, 3	8/2.1	Y	Y	Y	Y
OM-OW-R4	Review MOC		0, 1, 2, 3	8/2.2	N	N	N	N
OM-OW-R5	Develop an O&M Plan, issue for review and then issue for construction	Provide to Owner and DCO for review and update with comments	0, 1, 2, 3	6/13	Y	Y	Y	Y

9.3 Operation and Maintenance Phase Driller or Crew's (DCO) Activities

Tracking Number	*Operation and Maintenance Phase Driller or Crew's (DCO) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
OM-DCO-A1	Changes to the system software are managed in a controlled manner.	Per the MOC	0, 1, 2, 3	7/3.3i)	N	N	N	N
OM-DCO-A2	Impacts of the software change are to be reviewed for impact upon the system as a whole	Per the MOC procedure. If IL2 or IL3 function, notify ABS of the change.	2, 3	7/3.3ii), 7/3.3iii) & 8/3.1.1	Y	Y	Y	Y
OM-DCO-A3	Perform verification tests after upgrades or code changes (SI may perform peer reviews)	Peer review(s) of the code, at a minimum for IL2 or IL3	2, 3	8/3.3	N	N	N	N
OM-DCO-A4	Perform periodic software audits per the DCO schedule	Check Rev Tracking Numbers of installed software with the records to detect changes. Keep record of audit for review by ABS.	0, 1, 2, 3	---	N	N	N	N

Tracking Number	*Operation and Maintenance Phase Driller or Crew's (DCO) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
OM-DCO-R5	Update O&M Plan, as required	Acquire or develop missing or incomplete portions of the plan	0, 1, 2, 3	8/2	N	N	N	N
OM-DCO-R6	Review O&M plan		0, 1, 2, 3	8/2.1	N	N	N	N
OM-DCO-R7	Maintain ISQM integrated control system Software Register		0, 1, 2, 3	8/2.4	N	N	N	N
OM-DCO-R8	Maintain the Control Equipment Registry		0, 1, 2, 3	7/3.9	N	N	N	N
OM-DCO-A9	Monitor for obsolescence	Hardware & Software	0, 1, 2, 3	---	N	N	N	N

9.5 Operation and Maintenance Phase System Integrator's (SI) Activities

Tracking Number	*Operation & Maintenance Phase System Integrator's (SI) Activities*	*NOTES*	*IL Tracking Number*	*Ref*	*Provide to ABS*	*ABS Review*	*Provide to IA*	*IA Review*
OM-SI-R1	Deleted							
OM-SI-R2	Develop Operating Manual	Provide to Owner and DCO for review	0, 1, 2, 3	6/13	N	N	N	N

9.7 Operation and Maintenance Phase Subcontractors'(CT) Activities

None

9.9 Operation and Maintenance Phase Verification & Validation (V & V) Activities

None

9.11 Operation and Maintenance Phase Independent Auditor's (IA) Activities

None

APPENDIX **2**

Definitions and Abbreviations

1 Definitions *(1 September 2012)*

The following definitions are applied to the terms used in this Guide:

Adaptive maintenance: Modification of a software product performed after delivery to keep a computer program usable in a changed or changing environment.

Anomaly: The defect of concept error detected during the Verification process.

Artifact: A tangible product or by-product produced during the development of software. Some artifacts help describe the function, architecture, and design of software. Other artifacts are concerned with the process of development itself – such as project plans, business cases, and risk assessments. Much of what are considered artifacts is software documentation.

Canonical Data Model: The data model is designed to be clear to the user. It is to be unambiguous, verifiable and traceable. The model requires complete information and be consistent, as much as possible, throughout the project.

Change Control: Management of change as one part of the SCM process.

Closed Loop Verification: The inputs and outputs of the computer-based integrated system are to be simulated with minimal interaction of the other integrated components. The V & V may require changing register values of the program to evaluate the integrated control system software response. A comprehensive understanding of the software code and functions limits this option to simple systems.

Completeness: The state of software in which full implementation of the required functions is provided.

Component: One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components. Note: The terms "module," "component," and "unit" are often used interchangeably or defined to be sub-elements of one another in different ways depending upon the context. The relationship of these terms is not yet standardized.

Comprehensibility: The quality of being able to be understood; intelligibility, conceivability.

Concept Error: Where the interpretation of the ConOps is in error when compared to the SRS and SDS or FDD or where the intended purpose of the function was not described correctly leading to software modules not performing the intended function properly.

Concept of Operations (ConOps): ConOps is a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders.

Configuration Item: An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.

Consistency: Uniformity of design and implementation techniques and notation.

Corrective maintenance: Reactive modification of a software product performed after delivery to correct discovered faults.

Correctness: The state of software in which traceability, consistency, and completeness are provided.

Cosmetic Defects: These types of defects are the ones, which are primarily related to the presentation or the layout of the data. However there is no danger of corruption of data and incorrect values.

Critical Defects: These are extremely severe defects, which have already halted or are capable of halting the operation of the computer-based control system. Critical defects are also defects that are capable of unsafe operation of the EUC.

Defect: A software coding error.

Defect Classification: Defects are to be ranked based on the effect upon the system software, function IL rating and Human-Machine Interface. The SI, DCO and Owner are to rank the defects to prioritize the defects.

Deficiency: Where software appears not to be performing the functions as listed in the ConOps, SRS and SDS or FDD.

Degraded: A component or part of the control system or connected equipment is not functioning per the specification.

Design Group: A combination of the Concept and Requirement and Design Phases.

Driller or Crew Organization (DCO): The DCO is the user of the integrated system and is also the Duty Holder or drilling contractor. The DCO is also responsible for the Operation and Maintenance Phase of the system. Maintenance responsibility facilitates continued reliable operation of the integrated system as improvement, upgrades and new components are added to the system over its lifetime.

Emergency Maintenance: Unscheduled corrective maintenance performed to keep a system operational.

Emulator: An emulator duplicates the functions of one system using a different system. The second system "behaves" like the first system.

Essential Services: Services considered necessary for continuous operation to maintain propulsion and steering (primary essential services); non-continuous operation to maintain propulsion and steering and a minimum level of safety for the vessel's navigation and systems including safety for dangerous cargoes to be carried (secondary essential services); and emergency services as described in ABS *Steel Vessel Rules* 4-8-2/5.5 (each service is either primary essential or secondary essential depending upon its nature). Also refer to essential systems in 4-1-1/7 TABLE 3 and 4-1-1/7 TABLE 4 of the ABS *Rules for Building and Classing Mobile Offshore Drilling Units* and the ABS *Guide for the Classification of Drilling Systems.*

Failed: The ISQM control system or significant portions of the connected equipment is not functioning normally.

Failure Modes, Effects, and Criticality Analysis: The criticality analysis is used to chart the probability of failure modes against the severity of their consequences. The analysis highlights failure modes with relatively high probability and severity of consequences.

Firmware: The combination of a hardware device and computer instructions and data that reside as read-only software on that device.

Flexibility Matrix: A method that facilitates tradeoff analysis concerning scope, schedule and resources during project definition and work planning.

Function: The purpose of the equipment under control (i.e., the hydraulic power unit, winch, power management system).

Functional Design Document package: A collection of documents and/or drawings that describes the actions or functions of the control system, the interface to other integrated control systems, connected equipment functions (from other non-ISQM SI suppliers and sub-suppliers) and other pertinent information facilitating verification and integration, and for the Owner to manage the maintenance of the control system software.

Hardware: Physical equipment used to process, store, or transmit computer software or data.

Hardware-In-the-Loop Verification: The integrated system's program is being executed on its native hardware (CPU or controller hardware) and the simulation is being executed on a separate machine. Interfaces between the two are developed for the testing. The simulation is to be of sufficient fidelity to include physical real world dynamic systems to verify the central control system's programming and documenting the results of the stimulus. The real world represented by mathematical models in the simulation program.

Human Machine Interface: A display and operator input device.

Independent Auditor: This organization monitors involved parties, including Suppliers for compliance with this Guide, produces reports for the Owner, DCO & System Integrator. IL2 and IL3 rated functions are to have a third party IA. If one function is assigned an IL3, the Independent Auditor is to be an independent third party and the integrated control system carries an IL3 rating. IL0 and IL1 may have an IA from the Owner's, DCO's organizations or a third party. This person or team is to be independent from the concept and software development teams. If the Owner is taking the role as Independent Auditor, this group is to be an independent group under the Owner's umbrella. The IA may assist the Owner with validation of the system. During the V V&T Phase, the ConOps or the FDD document is reviewed to facilitate validation to the Owner's approved requirements. The Owner with input from the DCO and IA validates the control system.

Instrumentation: The attributes of software that provide for the measurement of usage or identification of errors.

Integrity Level: A number assigned by Owner and/or DCO to a computer-based function based upon the severity of the consequence of a failure of the function. Where 0 has little consequence to 3 where the consequence of a function failure is of significant concern with corresponding consequences.

Interoperability testing: Testing conducted to determine that a modified system retains the capability of exchanging information with systems of different types, and of using that information.

Major Defects: These are severe defects, which have not halted the system, but have seriously degraded the performance, caused unintended action or incorrect data transmitted.

Minor Defects: Defects which can or have caused a low-level disruption of function(s). Such defects can result in data latency but not in essential or IL2 or IL3 functions. The integrated system and the function continues to operate, although with a failure. Such a disruption or non-availability of some functionality can be acceptable for a limited period of time for IL1 functions. Minor defects could cause corruption of some none critical data values in a way that is tolerable for a short period.

Moderate Defects: A software function performs differently than specified in the SRS and SDS or FDD leading to a change in the Operating Manual, may be called a Moderate Defect. The Owner is to review the impact and risk of such a change.

Modification Request: A generic term that includes the forms associated with the various trouble/problem-reporting documents (e.g., incident report, trouble report) and the configuration change control documents [e.g., software change request (SCR)].

Modularity: Being provided with a structure of highly independent modules.

Native computer: The program is being executed on the hardware that it will execute upon when installed.

Non-native computer: The program is being executed on an emulation of the target hardware using an emulator.

Nonoperational: not in working order or ready to use.

Normal: The control system, connected components and associated input and output modules are in working order.

Operational: (1) Pertaining to a system or component that is ready for use in its intended environment. (2) Pertaining to a system or component that is installed in its intended environment. (3) Pertaining to the environment in which a system or component is intended to be used. (IEEE Std. 610, 1990, IEEE Standard Computer Dictionary, A Compilation of IEEE Standard Computer Glossaries)

Owner: The Owner is the organization which decides to develop the system, and provides funding.

Package: Hardware, software, sensors, wiring and appurtenances of an assembled unit.

Peer review: A process where a document or author's work is scrutinized by others who are competent or are considered experts in the same field.

Perfective maintenance: Modification of a software product after delivery to improve performance or maintainability.

Preventive Maintenance: Maintenance performed for the purpose of preventing problems before they occur.

Production Software: Software for a control system which is in use by the industry and where approximately 85% of the code or software modules are the same with customization of the configuration to meet the requirements or specifications.

Release Control: Transformation of configuration items into a deliverable asset.

Retirement: Withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system

Reverse Engineering: The process of extracting software system information (including documentation) from source code.

Safety: The ability of a system to avoid catastrophic behavior.

Self-Descriptiveness: The extent of a software's ability to provide an explanation of the implementation of a function or functions.

Ship Builder Integrator: The Ship Builder Integrator is the shipyard or the asset builder.

Simplicity: The provision of implementation of functions in the most understandable manner (usually avoidance of practices that increase complexity).

Software: Computer programs, procedures, test scripts and associated documentation and data pertaining to the operation of a computer system.

Software Design Specification: A document that describes the design of a system or component. Typical contents include system or component architecture, control logic, data structures, input/output formats, interface descriptions, and algorithms.

Software Maintenance: Modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.

Software Module: A smaller set of program code to carry out a logical subset of control action controlled by the over-riding program (i.e., A Software Module with program code to open a valve, monitor the valve that it did open and alarm if feedback is not provided within the prescribed time). Another example would be an analog loop where the main shaft is to rotate at 20 rpm and a closed loop control would adjust the drive's motor speed to maintain 20 rpm.

Software Requirements Specification (SRS): Documentation of the essential requirements (functions, performance, design constraints, and attributes) of the software and its external interfaces.

Software Risk: The potential loss due to failure during a specific time period.

Software-In-the-Loop Verification: The integrated system's program for the central control system is being executed on a non-native hardware and the simulation is being executed on the same or a separate machine. The simulation is to be of sufficient fidelity to include real world dynamic systems to verify the central control system's programming and documenting the results of the stimulus. The real world is represented by mathematical models in the simulation program.

System Integrator: The System Integrator is responsible for managing the development of the system, in charge of global design, integrating system elements and supplier management, as well as integration and verification of the whole system. The System Integrator may delegate certain responsibilities to suppliers and subcontractors where these delegated responsibilities are to be clearly defined. During some phases, the Integrator role may not be assigned to a dedicated organization, in those cases, the Integrator responsibility is assigned to one of the existing organizations: Owner, DCO or Supplier.

Systemic: Common element(s) (software routines or hardware) where a defect or failure of the element may cause cascading defects. A single 24VDC power supply could cause a systemic failure of the control system.

Testability: The ability of software to provide simplicity, modularity, instrumentation, and self-descriptiveness.

Traceability: The ability of software to provide a thread from the requirements to the implementation, with respect to the specific development and operational environment.

Unit Testing: A method wherein the smallest testable portions of a module are verified. Individual units are first tested then these are tested in combination with other units within the module to assess proper interactions and outcomes. Once the module has been proven then inter-module interactions can be tested.

V&V: Verification and Validation of the integrated software program.

V&V Organization: The V&V organization is to verify the functions defined in the Software Requirement Specification (SRS) and Software Design Requirement (SDS) or Functional Description Documents (FDD) using Closed Loop (specially considered), Software-In-the-Loop or Hardware-In-the-Loop

methodology. The V&V organization may be part of the System Integrator's organization or may be independent, as directed by the Owner, with limitation.

Validation: Determines if the software satisfy the intended use as documented in the ConOps.

Verifiability: The capability of software to be verified, proved, or confirmed by examination or investigation.

Verification: Demonstrate the software performs as delineated in the SRS and SDS or FDD. Also determines whether development products of a given activity conform to the requirements of that activity.

Version Control: Management of the asset versions generated as part of the SCM process.

Virus Definition: Database of computer virus signature used by anti-virus programs.

3 Abbreviations *(1 September 2012)*

The following definitions are applied to the terms used in this Guide:

ARMS : Accessibility, Reliability, Maintenance and Safety

BCS : Bulk Process Control System

BOP : Blowout Preventer

BPCS : Basic Process Control System

C : Concept Phase

CCB : Configuration Control Board

CCTV : Closed Circuit Television System

CI : Configuration Item or Software Module

CMMI : Capability Maturity Model Integration

CON : Construction Phase

ConOps : Concept of Operations document

COTS : Commercial Off The Shelf System

CPU : Central Processor Unit

CRT : Cathode Ray Tube

CT : Supplier, subcontractor and vendor Organizations

DCO : Driller or Crew Organization

DCS : Drilling Control System

DPCS : Dynamic Positioning Control System

EUC : Equipment Under Control

FDD : Functional Description Documents or package

FMEA : Failure Mode and Effects Analysis

FMECA : Failure Modes, Effects, and Criticality Analysis

FMS : Fluids Management System

FP : Function Point

HMI : Human Machine Interface

HPU : Hydraulic Power Unit

HW : Hardware

IA : Independent Auditor Organization

IEEE : Institute of Electrical and Electronics Engineers

IL : Integrity Level

I/O : Input/Output

ISQM : Integrated Software Quality Management

LOC : Lines Of Code

MOC : Management Of Change

MR : Modification Request

MTTF : Mean Time To Failure

O&M : Operation & Maintenance Phase

OW : Owner Organization

PHS : Pipe Handling System

PLC : Programmable Logic Controller to include single board computers

PM : Project Management

PMBOK® : Project Management Body of Knowledge

PMI : Project Management Institute

PMS : Power Management System

QHSE : Quality, Health, Safety and Environment

RAM : Random Access Memory

RD : Requirements and Design

SBI : Ship Builder Integrator

SCM : Software Configuration Management

SCMP : Software Configuration Management Plan

SCR : Software Change Request

SDD : Software Design Description

SDLC : Software Development Life Cycle

SDS : Software Design Specification

SI : System Integrator Organization

SIS : Safety Integrated System

SLOC : Source Lines of Code

SMS : Subsea Management System

SPMP : Software Project Management Plan

SQA : Software Quality Assurance

SRS : Software Requirement Specification

SWEBOK : Software Engineering Body of Knowledge

SY : Shipyard

V&V : Verification and Validation Organization

VMS : Vessel Management System

V V&T : Verification, Validation of and Transition Phase

WBS : Work Breakdown Structure

APPENDIX 3
Concept Phase

1 Example Concept of Operations Document *(1 September 2012)*

Preface, introduction, revision listing, table of contents

1) Scope of the Concept of Operations Document

a) To include:

i) System Overview (Extent of the ISQM system)

ii) Initial architectural design and associated preliminary drawings or sketches. (This is updated throughout the SDLC to become architectural design used for the control system)

iii) ISQM system description

iv) Definitions of IL risk terms

v) Identify potential new or novel functions, components, equipment or software code

vi) List of connected equipment

vii) Alarm Management Philosophy

viii) Control system data collection, as required

2) Control system integration details

a) Safety review(s) report(s) of the integrated system's functions

i) Listing of functions or equipment with assigned IL number

1) Identify if the function or equipment is new or novel technology

2) Identify if the function or equipment is an essential function or equipment

3) Example listing

a) Function 1 of supplier's equipment # 1

i) Function tracking identifier

ii) Function name

iii) Description

iv) IL number assigned

v) Fail safe state

b) Function 2 of supplier's equipment # 1

i) Function tracking identifier

ii) Function name

iii) Description

iv) IL number assigned

v) Fail safe state

c) Function n of supplier's equipment # 1

i) Function tracking identifier

ii) Function name

iii) Description

iv) IL number assigned

v) Fail safe state

d) Function of Equipment # 2 (single function)

i) Function tracking identifier

ii) Function name

iii) Description

iv) IL number assigned

v) Fail safe state

e) Continue with additional functions

b) ISQM system integration constraints

i) System Integrator's constraints by function

1) Function tracking identifier

2) Function name

3) IL number assigned

4) Constraint description

5) Resolution of any constraint(s), for the integrated system

ii) Suppliers' constraints by first: Function, second: Equipment

1) Function tracking identifier

2) Function name

3) IL number assigned

4) Constraint description

iii) Resolution of any constraint(s) for this function or connected equipment

3) ISQM Control System changes, updates, etc.

a) To existing system

i) Deletion of existing functions

ii) Expansion with additional functions

iii) Hardware expansion

b) Record why changes were made

4) ISQM control system verification method and suppliers of connected equipment verification

a) Primary verification method selected for the ISQM control system

b) Functions verification scenarios

i) Function tracking identifier

ii) Function name

iii) Function Description

iv) Operational and non-operational verification scenarios

1) Operational verification scenarios per Function

2) Degraded verification scenarios per Function

5) Suppliers package equipment

a) Supplier's Information

i) Function tracking identifier

ii) Manufacturer

iii) Model number of supplied equipment

iv) Interface protocol

1) Constraints with canonical integration model and resolution

v) Software data mapping and commands

1) Data map

a) Function's output data to ISQM control system

b) Function's inputs from ISQM control system

2) Commands

a) Functions' output to ISQM control system

b) Function's input from ISQM control system

3) Alarms

4) Design limits of equipment

a) NOTE: These are maximum and minimum pressure, temperature, weight…

5) Operating limits

a) NOTE: These are the maximum and minimum pressure, temperature, weight… for the function to operate under normal conditions within the design limits.

vi) Verification

1) Verification Report

a) A suppliers' verification report for all assigned IL1 and higher ISQM control system connected packages

b) ABS is to witness the verification process. Therefore, this part may be noted as "Witnessing required during verification process", and not supplied in the ConOps

c) Firmware version number and verified software version number and/or checksum of the program.

d) Verification report is to state verification method used (peer reviews, closed loop, etc.)

2) Verification Plan

a) Method used for verification (peer reviews, Software-In-the-Loop, HIL, other)

b) NOTE: Required for all IL2 and IL3 assigned connected equipment and associated functions

vii) Other information to facilitate integration

6) Human Machine Interface device

a) Supplier's Information

i) Function tracking identifier

ii) Manufacturer

iii) Model number of supplied equipment

iv) Interface protocol

1) Constraints with canonical integration model

v) Software data mapping and commands

1) Data map (if known at this time)

a) Function's output data to ISQM control system

b) Function's inputs from ISQM control system

2) Commands

a) Functions' output to ISQM control system

b) Function's input from ISQM control system

vi) Other information to facilitate integration

Appendices and glossaries to include references, as required.

3 Example Obsolescence Management Plan Outline

Title page

Revision chart

Preface

Table of contents

List of figures

List of tables

1) Scope
  1) Reason for Managing Hardware and Software Obsolescence
  2) Document overview
  3) Software Architecture Diagram
  4) Hardware Architecture Diagram
2) Referenced documents
3) Current system overview
  1) History of the integrated control system
  2) Metrics on the configuration management system
  3) Software Registry age of components distribution
  4) Hardware Registry age of components distribution
  5) PLC, workstation and server life cycle
  6) Support environment
4) Hardware Disposal
  1) QHSE Policies
  2) Tracking Policy
  3) Support in Disposal
5) Software Disposal
  1) Software License Issues
  2) Media Destruction
  3) Data Archiving

5 ConOps Traceability *(1 September 2012)*

The document is:

i) The foundation of traceability

ii) A common document for all stakeholders to agree upon the scope and functions using non-computer vocabulary. The functions are transliterated into software language in the RD Phase.

iii) The ConOps is to be a living document where it is updated with new information, constraints, safety review(s) recommendations and refined details

There are relationships between what the system is intended to do and what the system architecture indicates. As the Concept Phase progresses conflicts may arise between the planned functionality of different components of the system. Certain constraints and trade-offs are taken into consideration. Input from the Owner and DCO on desired functionality may involve tradeoffs affecting effort, schedule and maintainability of the control system. The reviews capture concerns and the experience from the interested parties.

The System Integrator (SI) will take the ConOps and develop the Software Requirements Specification (SRS) and Software Design Specification (SDS) documents with more detail for coding the Software Modules to control the functions. It is recommended that the Owner consider the ConOps as a technical bid document with sufficient detail to facilitate bidding and acceptance for the integrated system software development.

5.1 Example of Traceability Matrix

	Requirement Number and Description	*HW Module 1*	*HW Module 2*	*HW Module 3*	*HW Module 4*	*HW Module 5*	*HW Module 6*	*HW Module 7*
3.1	Functional Requirements							
3.1.1	Functional Requirement 1							
3.1.1.1	Introduction	x						
3.1.1.2	Inputs		x	x				
3.1.1.3	Processing							
3.1.1.4	Outputs							
3.1.2	Functional Requirement 2		x		x			
3.1.2.1	Introduction							
3.1.2.2	Inputs			x				
3.1.2.3	Processing		x		x			
3.1.2.4	Outputs							
3.1.n	Functional Requirement n		x					x
3.1.n.1	Introduction							
3.1.n.2	Inputs			x				
3.1.n.3	Processing	x						
3.1.n.4	Outputs	x	x					
3.2	External Interface Requirements	x						
3.2.1	User Interface							x
3.2.2	Hardware Interfaces	x	x	x	x			
3.2.3	Software Interfaces		x	x	x	x		
3.2.4	Communication Interfaces				x			
3.3	Performance Requirements							x
3.4	Design Constraints							x
3.4.1	Standards Compliance					x	x	
3.4.2	Hardware Limitations			x	x			

	Requirement Number and Description	*HW Module 1*	*HW Module 2*	*HW Module 3*	*HW Module 4*	*HW Module 5*	*HW Module 6*	*HW Module 7*
3.5	Quality Characteristics							
3.5.1	Correctness	x						x
3.5.2	Unambiguous		x				x	
3.5.3	Completeness			x		x		

APPENDIX 4

Requirements and Design Phase

1 Software Requirements Specification

(1 September 2012) The ISQM SRS is a specification for the integration of a defined set of functions consisting of particular software products, programs, or set of programs that perform defined functions in a defined environment. It is recommended that the SI lead meetings involving the Owner and/or DCO in SRS development. The basic issues that the SRS addresses are the following:

- *Functionality:* What is the software supposed to do?
- *External interfaces:* How does the software interact with people, the system's hardware, other hardware, and other software?
- *Performance:* What is the speed, availability, response time, recovery time of various software functions, etc.?
- *Attributes:* What are the portability, correctness, maintainability, security, etc. considerations?
- Design constraints imposed on an implementation.
- Are there any required standards in effect, implementation language, policies for database integrity, resource limits, operating environment(s), etc.?

Avoid placing either design or project administration or schedule requirements in the SRS.

Software requirements specification (SRS): Documentation of the essential requirements (functions, performance, design constraints, and attributes) of the software and its external interfaces.

1.1 Example of Software Requirements Specification Table of Contents

1. Introduction
   - 1.1 Purpose
   - 1.2 Scope
   - 1.3 Definitions, acronyms, and abbreviations
   - 1.4 References
   - 1.5 Overview
2. Overall description
   - 2.1 Product perspective
   - 2.2 Product functions
   - 2.3 User characteristics
   - 2.4 Constraints
   - 2.5 Assumptions and dependencies
3. Specific requirements

3.1 External interface requirements
3.1.1 User interfaces
3.1.2 Hardware interfaces
3.1.3 Software interfaces
3.1.4 Communications interfaces

3.2 Functional requirements
3.2.1 Mode 1
3.2.1.1 Functional requirement 1.1
3.2.1.n Functional requirement 1.n
3.2.2 Mode 2
3.2.m Mode m
3.2.m.1 Functional requirement m.1
3.2.m.n Functional requirement m.n

3.3 Performance requirements

3.4 Design constraints

3.5 Software system attributes

3.6 Other requirements

Appendixes

Index

3 Software Design Specification

An ISQM Software Design Document (SDD) is a written description of a software product integration, that a software designer writes in order to give a software development team an overall guidance of the architecture of the software integration project. A SDD usually accompanies an architecture diagram with pointers to detailed feature specifications of smaller pieces of the design. Practically, a design document is required to coordinate a large team under a single vision. A design document needs to be a stable reference, outlining all parts of the software and how they will work. The document's goal is to give a fairly complete description, while maintain a high-level view of the software.

Software design specification (SDS): A document that describes the design of a system or component. Typical contents include system or component architecture, control logic, data structures, input/output formats, interface descriptions, and algorithms.

3.1 Example of Software Design Specification Table of Contents

1.0 Introduction

1.1 System Overview

1.2 Design Considerations

1.3 Assumptions and Dependencies

2.0 General Constraints

Hardware or software environment

End-user environment

Availability or volatility of resources

Standards compliance

Interoperability requirements

Interface/protocol requirements

Data repository and distribution requirements

Security requirements

Memory and other capacity limitations

Performance requirements

Network communications

Verification and validation requirements (testing)

Other means of addressing quality goals

Other requirements described in the requirements specification

2.1 Goals and Guidelines

2.2 Development Methods

3.0 Architectural Strategies

3.1 strategy-1 name or description

3.2 strategy-2 name or description

...

4.0 System Architecture

4.1 component-1 name or description

4.2 component-2 name or description

...

5.0 Policies and Tactics

5.1 policy/tactic-1 name or description

5.2 policy/tactic-2 name or description

...

6.0 Detailed System Design

6.1 module-1 name or description

6.2 module-2 name or description

...

Glossary

Bibliography

5 Models

The R & D phase also includes the development of several models at different levels as required by the control systems complexity. The quality criteria are driving factors that are incorporated in the following models:

- Owner-level models that map to Owner level principles and objectives are developed to provide documentation of the relationship between Owner's objectives and the system/software.
- User-level models depict user-level criteria and principles. Owner-level and user-level models can be compared to identity any conflict.
- Developer-level models are developed using some of the same principles and criteria

The models are tools as they are inputs to Work Process Flow Diagrams, Entity-Relationship Diagrams, Data Flow Diagrams, Implementation Strategy, a Canonical Data Model, etc. These artifacts may or may not be constructed depending on the complexity of the project, the requirements of the chosen SDLC, the level of automation of the SI team or the perceived benefit of detailed architectural and design documentation.

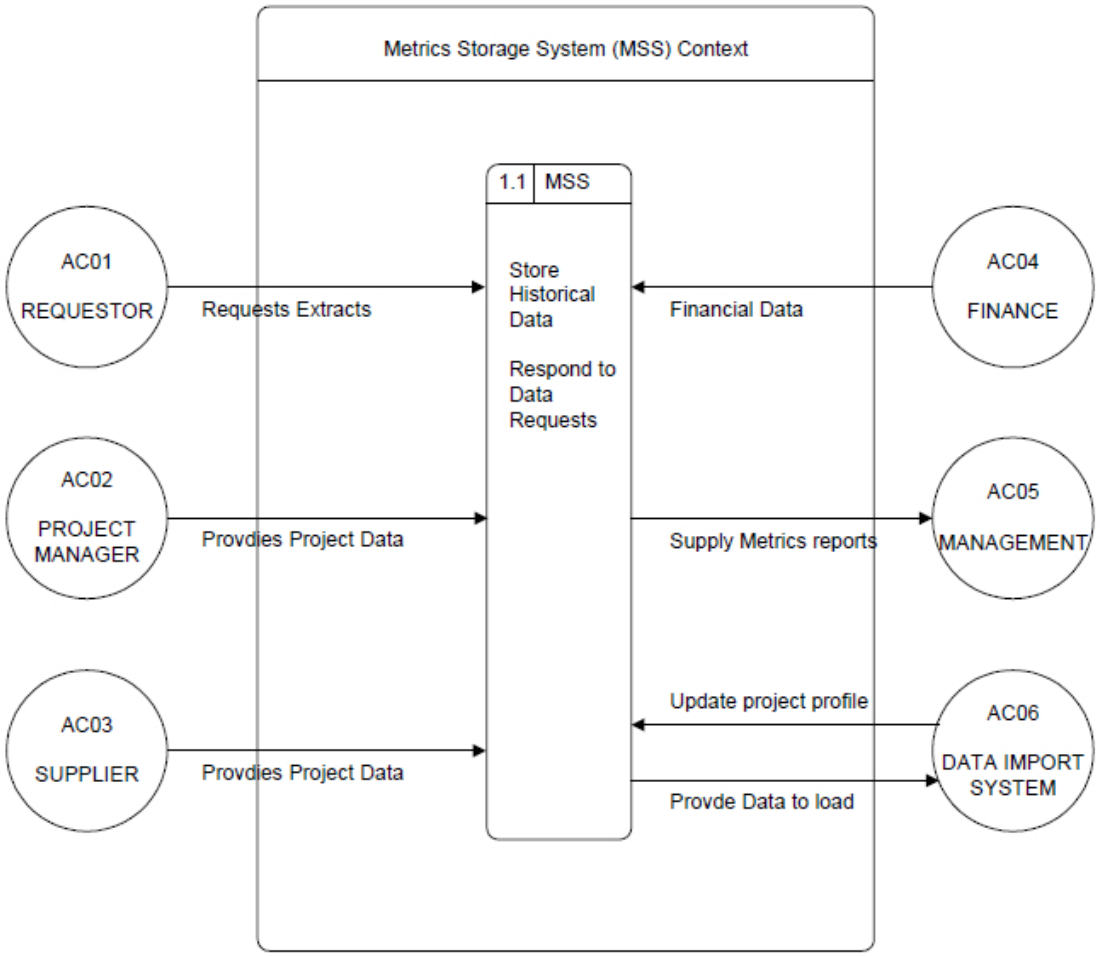
5.1 Models

5.1.1 Owner Level Models

Two examples of Owner-level models are shown below: the System Context model and the Current System model. Owners generally do not develop these models. The development group (architects and analysts) develops the models based on Owner's input. Once complete the development group confirms the accuracy of the models with the Owner.

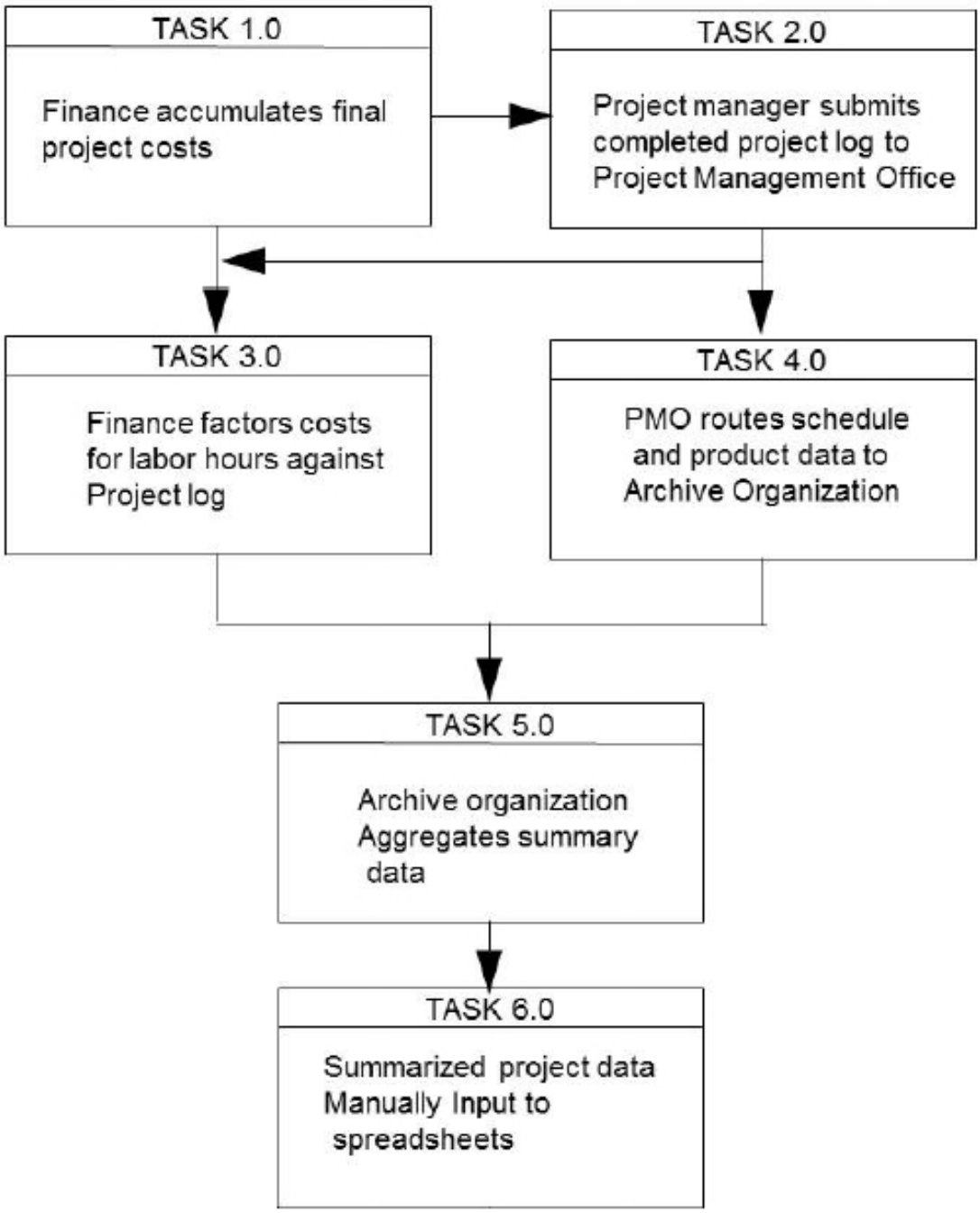
A4/5.1.1 FIGURE 1 is an example of an Owner-level system context model for one process within a system. It is a very basic model that is used to clarify Owner understanding of relationships within a system. There may be many context diagrams in a system, depending on the complexity.

FIGURE 1



A4/5.1.1 FIGURE 2 is an example of a Current System model that describes a manual system for capturing and storing historical data. This Owner-level model is used to determine that functions in the current system which are retained in a new system, are not overlooked.

FIGURE 2

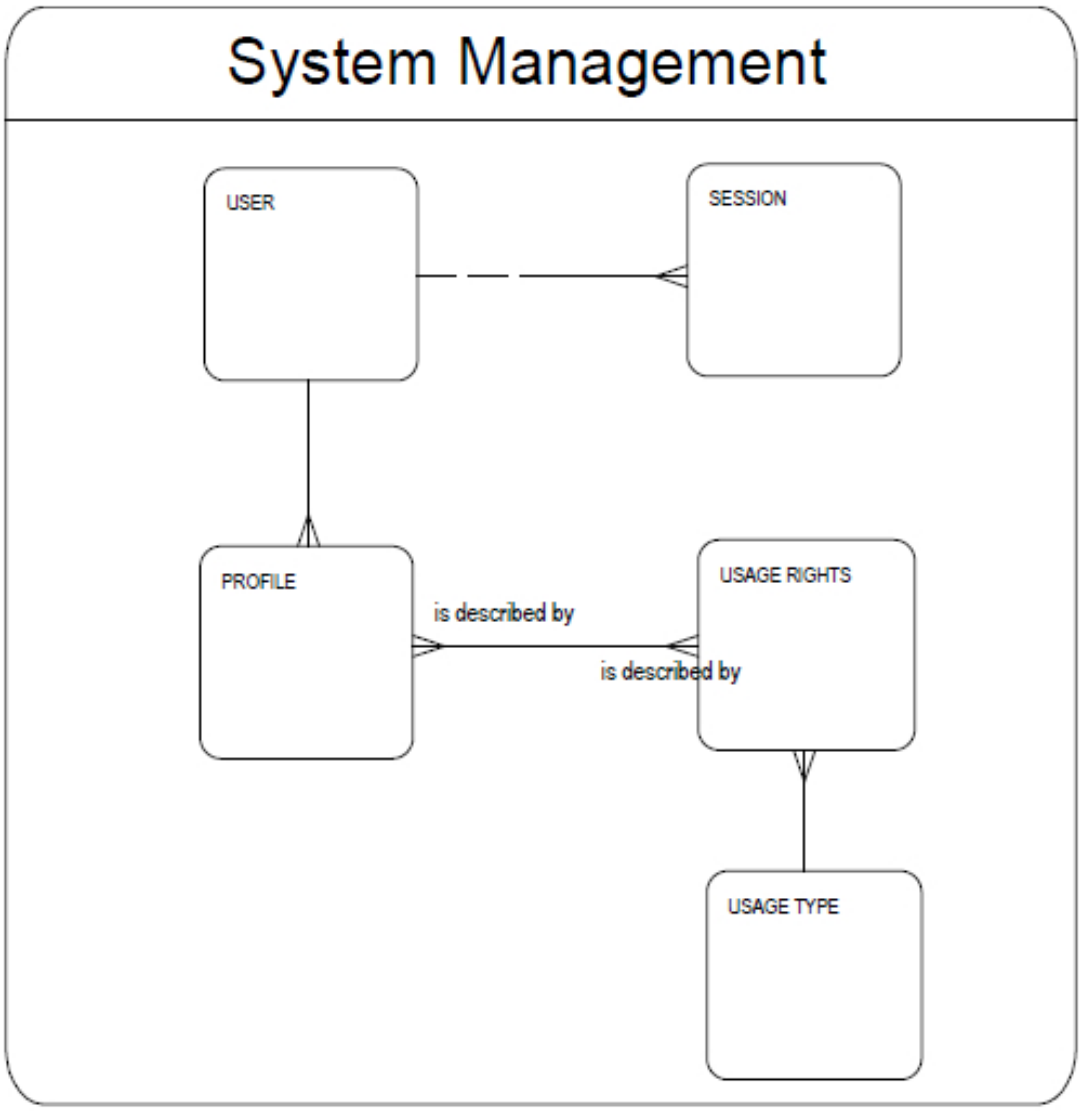


5.1.2 User Level Models *(1 September 2012)*

Three examples of user-level models are shown below; the entity-relationship model, the functional model and the work process model. Users generally do not develop these models; the development group (architects and analysts) develops the models based on user input. Once complete the development group confirms the accuracy of the models with the DCO.

A4/5.1.2 FIGURE 3 is an example of a user level Entity-Relationship Model titled System Management. The entities are depicted by the "roundtangle" and the relationship is depicted by the connecting lines; multiple tails indicate many options, a single tail means a single option. For example, the entity "User" has a single "Profile", but "Profile" describes multiple users.

FIGURE 3

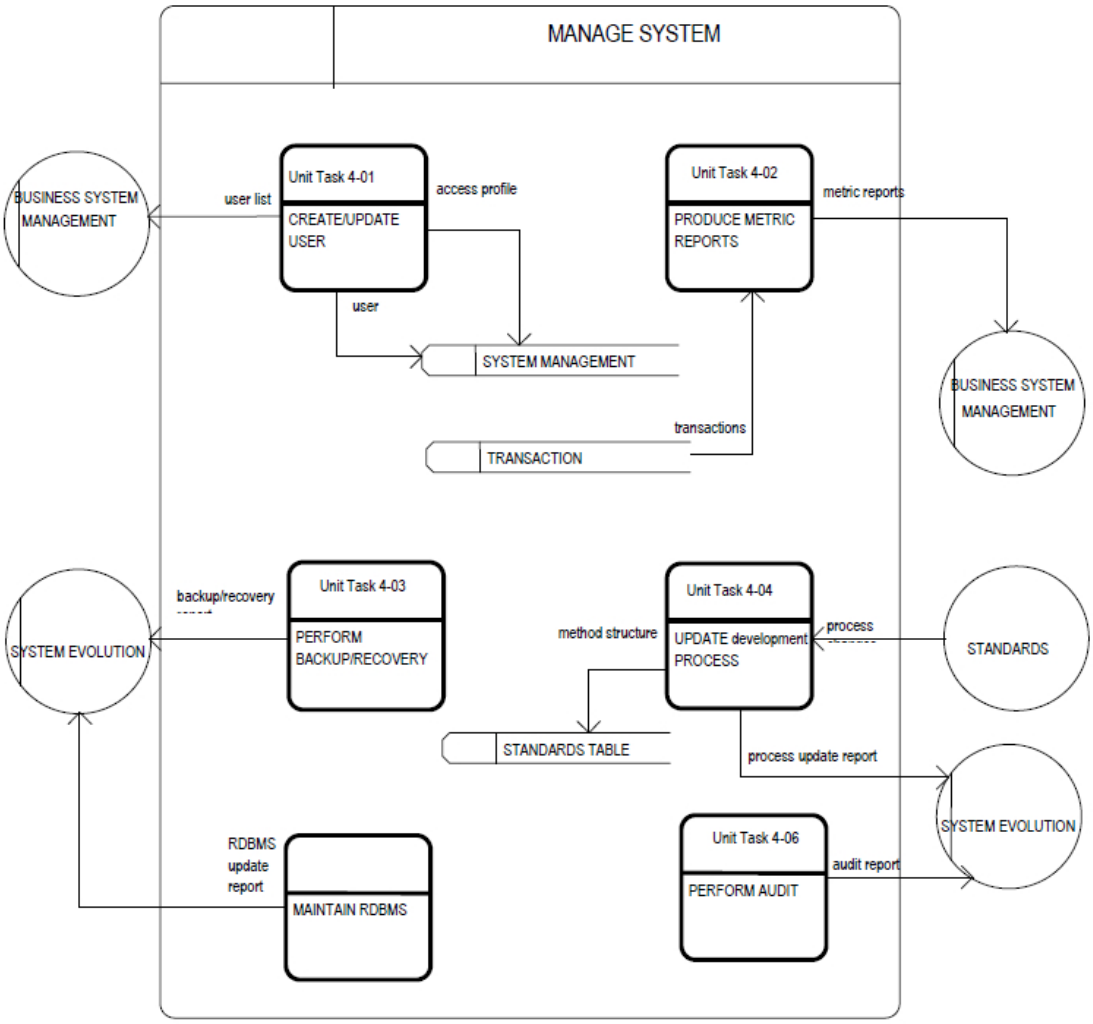


A4/5.1.2 FIGURE 4 is an example of a user level Functional Model titled Manage System. This model is also sometimes called a Conceptual Data model. The tasks that are to be performed by the user are shown in the “roundtangles” and the entities they relate to are depicted by:

- Circles if they are outside the function; if the circle has a vertical line inside, the entity is internal to the system, otherwise it is external such as the entity “Standards”
- “Longtangles” if the entities are internal to the system, such as a database called “Standards Table”.

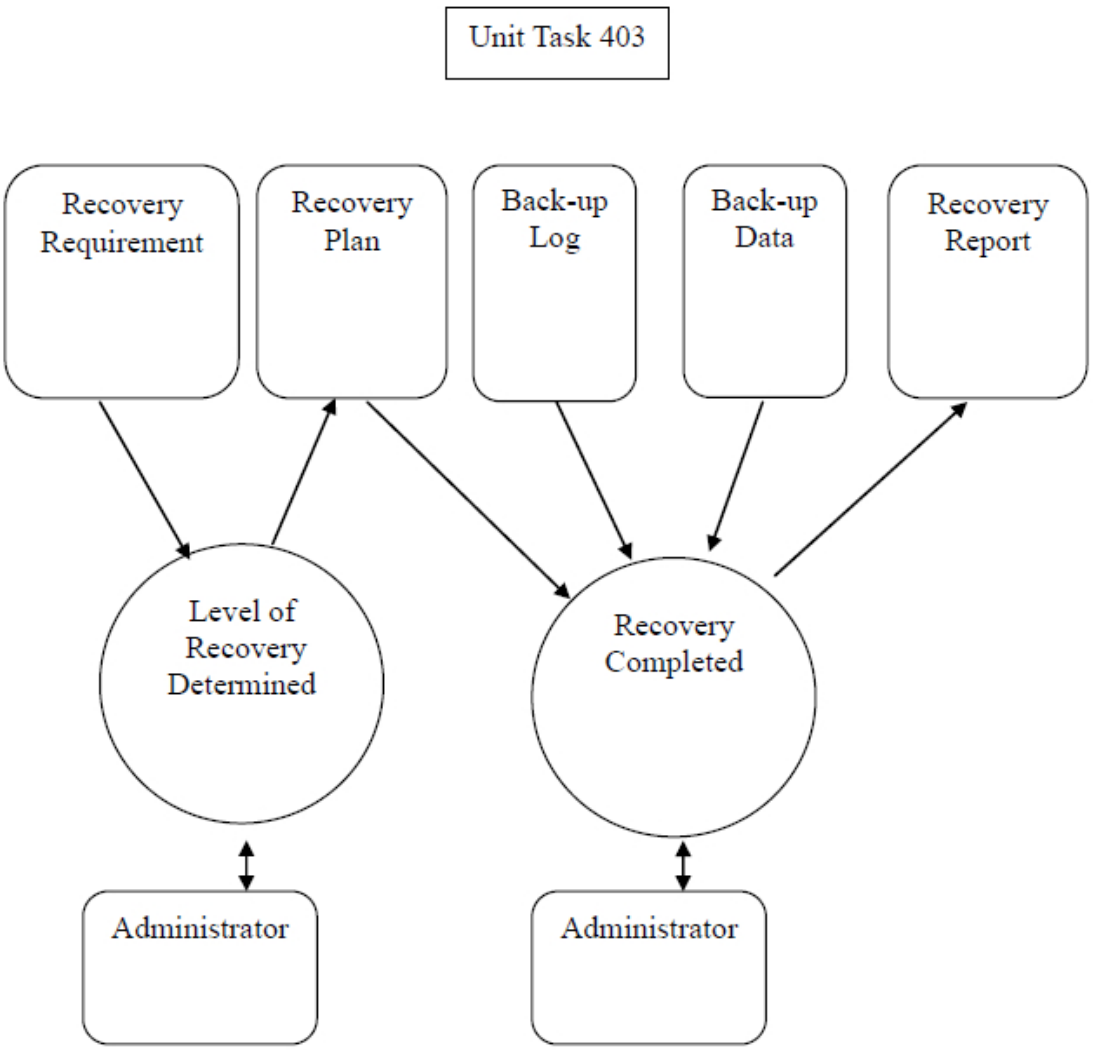
Inputs and outputs are noted by plain text.

FIGURE 4



A4/5.1.2 FIGURE 5 is an example of a user level Work Process Flow Model. Note that it relates to Unit Task 4-03 in A4/5.1.2 FIGURE 4. The model denotes the actors in the process in the lower row, the action that occurs in the middle row and the artifacts (physical and virtual) that are involved.

FIGURE 5

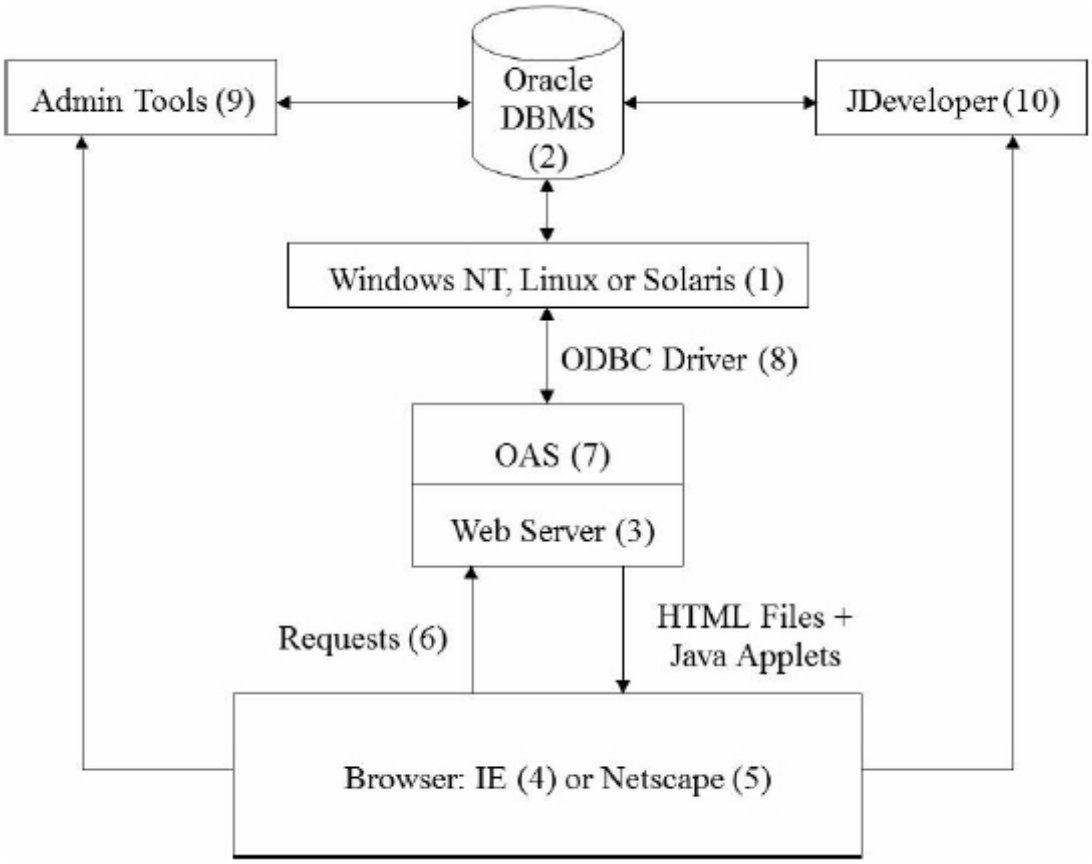


5.1.3 Developer Level Models

Two examples of developer-level models are shown below; the Software Architecture model and the Technology and Distribution model.

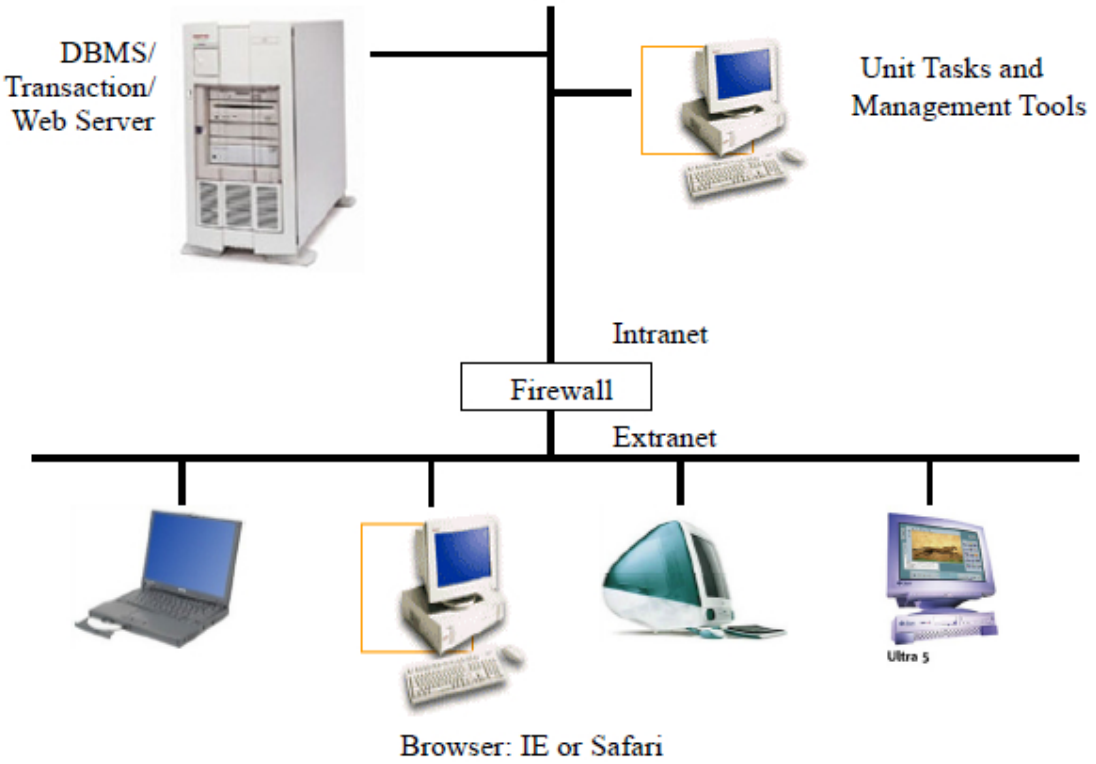
A4/5.1.3 FIGURE 6 is an example of a developer-level System Architecture model depicting the information system components required by the architecture.

FIGURE 6



A4/5.1.3 FIGURE 7 is an example of a developer-level Technology and Distribution model depicting the infrastructure linkages and high level operation.

FIGURE 7


DBMS/
Transaction/
Web Server
Unit Tasks and
Management Tools
Intranet
Firewall
Extranet
Ultra 5
Browser: IE or Safari

APPENDIX 5

Construction Phase

(1 September 2012) The Construction phase develops and implements the integration code of the functions that executes the SRS requirements. Because of the control system software development and testing in this phase, most documents previously developed are modified. This is the phase where the majority of changes may occur. It is recommended that the configuration management process be defined and implemented before or at the beginning of the Construction Phase.

The Construction Phase consists of the SRS and SDS or FDD refinement, coding of the Software Modules, integration of COTS products' configuration, unit testing, integration testing, and software system level acceptance testing is performed in the Construction Phase. The following are maintained under configuration management in the Construction Phase:

i) Errors or clarifications identified in the SRS and SDS or FDD are corrected, reviewed and approved by the Owner before code is written.

ii) The SI is to provide a document attesting that all SI developed Software Modules have been reviewed and unit tested.

iii) Once units of integrated Software Modules are reviewed, they are to be placed under configuration management and integrated into the baseline project.

iv) It is recommended that integration testing is performed each time a Software Module is integrated into the baseline to verify that it interfaces correctly with the remainder of the software.

v) After all individual Software Modules have been successfully incorporated, an overall software system level SI integration test is performed to verify that the software satisfies the requirements of the SRS and SDS or FDD.

vi) At the completion of the Construction Phase, the SI is to provide a test summary report.

1 Software Coding and Testing

The SI and V & V organizations develop and maintain, under configuration management, the following:

i) Traceability to the requirements and design of the software item (SI)

ii) Documented consistency with the requirements and design of the software item (SI)

iii) Documented consistency between unit requirements, canonical integration model (SI)

iv) Development and maintenance of all test scripts and data sets (V&V or SI)

v) Development of regression test suites (V&V or SI)

vi) Documented test coverage of units (V&V or SI)

vii) Documented feasibility of software integration and testing (V&V or SI)

viii) Documented feasibility of operation and maintenance (SI)

1.1 Software Integration *(1 September 2012)*

The SI and V & V organizations develop and maintain, under configuration management, the following:

i) The integration plan includes test requirements, procedures, data, responsibilities and schedule. The integration plan is a section of the V&V Plan. (V&V or SI)

ii) Each requirement is to be supported by a set of tests, test cases and test procedures for the integration testing. (V&V or SI)

iii) It is recommended that each test case be documented and traceable to the requirement(s) in the SRS and SDS or FDD.

1.3 Software SI Integration Testing

The SI and V & V organizations develop and maintain, under configuration management, the following:

i) Test coverage of the requirements of the software item (SI)

ii) Conformance to expected results (SI)

iii) Feasibility of software acceptance testing (V&V or SI)

iv) Feasibility of operation and maintenance (SI)

The following is an example of the software configuration management plan developed to manage the documents and software developed for the integrated software control system.

Example Software Configuration Management Plan (SCMP)

Software Configuration Management Plan

for

<Name of Project>

<author>

<date>

Version	Release Date	Responsible Party	Major Changes
0.1			Initial Document Release for Comment

3 Management

This section describes the organization, and associated responsibilities.

3.1 Organization

This subsection describes the organizational structure that influences the configuration management of the software during the development and the operation and maintenance phases.

i) Describe each major element of the organization together with the delegated responsibilities. Organizational dependence or independence of the elements responsible for SCM from those responsible for software development and use be clearly described or depicted.

ii) Include an organizational chart or list for the project that illustrates the structure for program/ project/ system management.

iii) Describe the organization responsible for SCM during the operation and maintenance phase.

iv) Describe the interface between the developing organization and the using organization, if any, with particular emphasis on the transfer of SCM functions in the operations and maintenance phases

v) Specifically cover the organizational relationships with the Configuration Control Board in the development and the operation, and maintenance phases.

3.3 Software Configuration Management Responsibilities

This subsection describes:

i) The organizational responsibilities for each Software Configuration Management (SCM) task; for example, identification, control, status accounting, and reviews and audits.

ii) The relationships with software quality assurance, software development, and other functional organizations ensuring delivery of the approved final product configuration.

iii) The responsibilities of the users and developer/maintenance activity in the review, audit, and approval process during each phase of the life cycle.

iv) Any SCM responsibilities of the representatives from each organization participating in the product development.

v) The overall responsibility of the Configuration Control Board (CCB).

vi) Any unusual responsibilities such as special approval requirements necessary to meet SCM requirements.

3.5 Software Configuration Management Plan Implementation

This subsection establishes the major milestones for implementation of the SCMP. Example milestones include the establishment of:

i) The configuration control board

ii) Each configuration baseline

iii) Schedules and procedures for SCM reviews and audits

iv) Configuration management of related software development, test, and support tools.

3.7 Applicable Policies, Directives, and Procedures

This subsection includes:

i) Identify applicable SCM policies, directives, and procedures.

ii) Develop SCM policies, directives, and procedures for inclusion for this project.

Examples of material which may be covered by policies, directives, and procedures are:

i) Identification of levels of software in a hierarchical tree

ii) Program and module naming conventions

iii) Version level designations

iv) Software product identification methods

v) Identification of specifications, test plans and procedures, programming manuals, and other documents

vi) Media identification and file management identification

vii) Document release process

viii) Turnover or release of software products to a library function

ix) Processing of problem reports, change requests, and change orders

x) Structure and operation of configuration control boards

xi) Release, and acceptance of software products

xii) Operation of software library systems to include methods of preparing, storing, and updating modules

xiii) Auditing of SCM activities

xiv) Problem report, change request or change order documentation requirements describing purpose and impact of a configuration change, or both

xv) Level of testing required prior to entry of software into configuration management

xvi) Level of quality assurance; for example, verification against development standards, required prior to entry of software into configuration management.

5 SCM Activities

This section describes how the following requirements for SCM are satisfied:

i) Configuration identification

ii) Configuration control

iii) Configuration status accounting and reporting

iv) Configuration audits and reviews

5.1 Configuration Identification

This subsection describes:

5.1.1

Identify the software project baselines (that is, the initial approved configuration identifications) and correlate them to the specific life-cycle phases. For each baseline, the following are described:

i) The items which form each baseline (for example, software requirements specifications, deliverable software, etc.).

ii) The review and approval events and the acceptance criteria associated with establishing each baseline.

iii) The users' and developers' participation in establishing baselines.

Elements of a baseline definition might include the following:

i) Product name and nomenclature

ii) Product identification number

iii) For each new version release, the version release number, a description of the new changes, the change release vehicle, the changes to any support software, and the changes to the associated documentation.

iv) Installation instructions

v) Known faults and failures

vi) Software media and media identification

5.1.2

Delineate the project titling, labeling, numbering, and cataloging procedures for all software code and documentation.

5.3 Change Control

This subsection describes:

5.3.1

Identify the routing of change proposals during each of the software life cycle phases. This may be provided in chart form with narrative support.

i) Describe the methods of implementing approved change proposals (to include changes in source and object code, and documentation).

ii) Describe the procedures for software library control including those procedures that provide for:

- Access control
- Read and write protection for applicable baselines
- File protection
- File identification
- Archive maintenance
- Change history
- Disaster recovery

iii) If patches are used to change object code, describe the methods for identification and control.

5.3.2

Define the role of each; for example, change review authority

i) Specify their authority and responsibility

ii) Identify the chairperson and the membership in the organizations, if the organizations have been formed

iii) State how the chairperson and the members (and alternates) are to be appointed, if the organizations have not yet been formed

iv) State the relationships of the developers and the users to the CCB(s)

5.5 Configuration Status Accounting

This subsection details:

i) Describe how information on the status of configuration items is collected, verified, stored, processed, and reported.

ii) Identify the periodic reports to be provided, and their distribution.

iii) State what dynamic inquiry capabilities, if any, are provided.

iv) Describe the means to be used to implement any special status accounting requirements specified by the user.

Some examples of information normally desired are as follows:

- Status of specifications
- Status of proposed changes
- Reports of approved changes
- Status of product versions or revisions
- Reports of the implementation of installed updates or releases
- Status of user-furnished property; for example, user-furnished operating systems

5.7 Audits and Reviews

This subsection details:

i) The SCM role in audits and reviews to be performed at specified points in the software life cycle defined in 1.2 of the SCMP.

ii) Identify the configuration items covered at each of the audits and reviews.

iii) State the procedures used for the identification and resolution of problems occurring during these audits and reviews

7 Tools, Techniques, and Methodologies

This section identifies and states the purposes, and describes (within the developers' scope of proprietary rights) the use of the specific software tools, techniques, and methodologies employed to support SCM on the specific project. This includes the tools, techniques, and methodologies used to:

i) Identify software media and media documentation

ii) Bring documentation and media under SCM control and formally release it to a user

iii) Document the status of changes made to software and associated documentation. It further defines the tools, methodologies, and techniques to be used to prepare reports for various levels of management, such as the project manager, CCB, SCM, and the user.

9 Supplier Control

This section states the provisions for assuring that vendor-provided and subcontractor-developed software meet established SCM requirements.

i) Indicate the proposed methods for control of subcontractors and vendors insofar as it impacts on the execution of this SCMP.

ii) Explain the methods to be used:

- To determine the SCM capability of subcontractors and vendors
- To monitor their adherence to the requirements of this SCMP

At a minimum, the supplier is to prepare and implement a SCM plan.

11 Records Collection and Retention

This section describes:

i) Identify the SCM documentation to be retained

ii) State the methods and facilities used to assemble, safeguard, and maintain this documentation. As part of this, identify any off-site backup facilities used

iii) Designate the retention period

APPENDIX 6

Verification, Validation and Transition Phase

1 Example V&V Plan Outline *(1 September 2012)*

The user may adapt any logical format desired for the V&V plan. The plan developer is to include traceability in the plan to trace functions back to the SRS.

Example Software V & V Plan Outline

1. Purpose of the V&V Plan
   - 1.1 Extent of the V&V Plan or envelope of testing
2. Referenced Documents for the V&V Plan
3. Definitions of terms used in the V&V Plan
4. V & V Plan for Control System
   - 4.1 Description of overall testing of the control system to include:
     - 4.1.1 Data collection or monitoring of the control system functions to detect failures of Software Modules functions
     - 4.1.2 Alarm monitoring
     - 4.1.3 HMI performance

5. V & V Plan for Control System Functions

5.1 Function 1 (from the SRS and SDS or FDD)

5.1.1 Function tracking identifier

5.1.2 Function name

5.1.3 Description of function

5.1.4 IL number assigned

5.1.5 Fail safe state

5.1.6 Operation verification scenario details

5.1.7 Non-operational verification scenarios

a) Non-operational verification scenario #1 details

a.1) Non-operational verification scenario expected results

a.2) List all expected results based upon other scenarios in the V&V Plan

b) Non-operational verification scenario #2 details

b.1) Non-operational verification scenario expected results

b.2) List all expected results based upon other scenarios in the V&V Plan

c) Continue until scenarios listed in the SRS and SDS or FDD are detailed.

5.2 Function 2 (from the SRS and SDS or FDD)

5.2.1 Function tracking identifier

5.2.2 Function name

5.2.3 Description of function

5.2.3 IL number assigned

5.2.4 Fail safe state

5.2.5 Operation verification scenario details

5.2.6 Non-operational verification scenarios

a) Non-operational verification scenario #1 details

a.1) Non-operational verification scenario expected results

a.2) List all expected results based upon other scenarios in the V&V Plan

b) Non-operational verification scenario #2 details

b.1) Non-operational verification scenario expected results

b.2) List all expected results based upon other scenarios in the V&V Plan

c) Continue until scenarios listed in the SRS and SDS or FDD are detailed.

5.n Function n (from the SRS and SDS or FDD, continue until all functions listed)

6. V&V Plan for Overall Verification of Integration of Components

6.1 Integrated Component # 1

6.1.1 Integration testing

6.2 Integrated Component # 2

6.2.1 Integration testing

6.n Integrated Component # n

6.n.1 Integration testing

3 Grouping of Software Modules

Grouping of the Software Modules into integration groups allows for components to be designed, built and tested together. Aligning integration groups with user processes permits test conditions that can simulate the use of the system when in production. If multiple integration teams will develop parts of the release, or the system is large, collections of integration groups can be organized into sub-releases. Sub-releases can then be assigned to individual development teams or simply used as a basis for subdividing a large design and construction effort for planning purposes.

The successive iterations of test and integration groups leads the system, or release, to the state in which it is entirely tested, thus triggering the preparation of V V&T testing. Based on the quality criteria and explicit acceptance criteria, the developer along with the user prepares the acceptance groups and test cases the same way the tester prepared the integration test cases. The acceptance testing specifications are refined here, but their actual execution is part of the V V&T phase.

APPENDIX 7

Operation and Maintenance Phase

All software requires maintenance. It is especially true of embedded software running on a PLC device. Even if no defects are detected, all software is to be updated over time to:

- Adjust to changes in external interfaces,
- Upgrade and/or replace obsolete versions of third party components
- Be moved to a new computing platform when the original one becomes unserviceable or inadequate
- Make minor modifications to the functionality to address new requirements, or needs, that were overlooked during initial system development

Configuration management keeps the documentation synchronized with the functional and physical characteristics of the system.

It is recommended that any information that may be needed in the future for any aspect of operation, maintenance, retirement, or replacement are recorded and kept up-to-date.

1 Recommended ISQM Maintenance Personnel's Activities

a) Managing the End of Life Plan for each Programmable Logic Controller (PLC), Human Machine Interface (HMI), and software component

b) Maintaining the Software Register

c) Ensuring adherence to Software Configuration Management policies and procedures

d) Reviewing Alarm Databases to detect significant events and anomalies, monitor hazardous trends, adherence to Alarm Management Policies and to proactively address issues

e) Fixing PLC code and triaging problems by interacting with Equipment Vendors

f) Carrying out inspections and maintenance on electronic equipment

g) Assisting with the implementation of audit recommendations

h) Ensuring that reports for maintenance and repair are accurate and complete

i) Assisting in installation, calibration, and modification to electronic systems

j) Informing supervisors and other department heads of any technical problems or limitations that may affect the safe operation of the system

k) Assisting in providing information related to the maintenance and repair budget

l) Responding to emergency situations as per designated policy

m) Assisting with incident investigation

n) Assisting with preparation of Job Safety Analysis for hazardous situations

o) Reporting any incidents, potential hazards or abnormal situations

p) Ensuring adherence to all relevant safety procedures and practices

q) Participating in weekly safety meetings and pre-job meetings, as required

r) Carrying out assigned duties in a safe manner, according to Company policies and procedures

3 Example O & M Plan Table of Contents

3.1 Example of Maintenance Plan

Maintenance Plan outline derived from Annex C, IEEE Std 1219-1998, Software Maintenance.

1. Introduction

2. References

3. Definitions

4. Software Maintenance Overview

4.1 Organization of members

4.2 Scheduling priorities

4.3 Resource summary, as required

4.4 Responsibilities of team members

4.5 Other

4.5.1 Tools

4.5.2 Techniques

4.5.3 Methods for execution of activities

5. Software Maintenance Process

5.1 Problem, modification identification, classification, and prioritization of issues and modifications

5.2 Analysis of the proposed software change

5.3 Design issues

5.4 Implementation of the proposed change

5.5 Verification or system testing

5.6 Validation or acceptance testing

5.7 Installation of the software (delivery)

6. Reporting Requirements for software maintenance

7. Administrative Requirements for software maintenance

7.1 Reporting of detected anomaly subsequent resolution

7.2 Requirements for deviations

7.3 Control Procedures

7.4 Standards, practices, and conventions to be followed

7.5 Performance tracking (optional)

7.6 Quality control plan for software revisions and revisions to this procedure or plan

8. Additional documentation required for software maintenance

3.3 Example of Operation and Maintenance Plan Outline *(1 September 2012)*

O&M Plan outline derived from IEEE Std 14764-2006.

i) Overview

1) Describe the system to be maintained

2) Identify the current status of the system and an overview of the software and hardware maintenance to date

3) Identify the IL2 and IL3 components to be maintained

4) Define the maintainer/support organization

5) Identify the hardware and software maintenance life cycle for the system

6) Identify the contract standards applied

7) Identify maintenance locations (e.g. on the vessel, in the lab at the factory).

ii) Plan Management of Change

1) Define the management of change process applied to this plan.

2) Specifically identify all plan stakeholders and their contributions to the maintenance activities.

iii) References

1) Identify all previously produced and maintained documentation for the system under maintenance.

2) Identify all equipment vendor sources of documentation and produce the current versions of all applicable hardware and software documentation

3) List all vendor, subcontractor and Owner/DCO contacts for the system under maintenance.

iv) Definitions

1) Define or reference all terms required to understand the maintenance plan

2) Describe all abbreviations and notations used

v) Maintenance Organization activities

1) Maintainer activities before the start of maintenance

a) Hardware and Software Process Definition

b) Establish Maintenance Infrastructure

c) Develop the maintenance plan identifying all resources required: facilities, laboratories, people, budget, etc.

2) Activities during maintenance

a) Monitor maintenance activities to conform to standards and life cycle processes

b) Develop the installation plan

c) Develop and execute regression testing of all changes

d) Interface with other stakeholder organizations

3) Post-Delivery roles and responsibilities of the maintainer

a) Post-Delivery process update and improvement

b) Problem Analysis and resolution

c) Maintenance review/acceptance

d) Update Migration Planning

e) Update Asset Retirement Planning

4) Role of the Owner/DCO

a) Acceptance testing

b) Re-class of asset, as required

vi) Define Resources for Maintenance

1) Personnel

a) Size of staff for the project

2) Software

a) Identify all software to be maintained on the vessel. This is the Vessel Software Registry.

b) Identify software needed to support the integrated control system

3) Hardware

a) Identify all hardware that hosts the integrated software control system. This is the Vessel Hardware Registry.

b) Identify hardware needed to support the integrated control system

4) Facilities

a) Identify facilities requirements

5) Special procedural requirements (e.g., security, access rights, and documentation control)

6) Describe the cost estimating method

7) Documentation to be updated

a) Software Quality Plan

b) Project Management Plan

c) Configuration Management Plan

d) Maintenance manuals

e) Regression Testing Plan

f) Training Plan

g) User's Manual(s)

vii) Training

1) Identify training needs of the maintainer and users

viii) Software maintenance control requirements

1) Describe the deviation policy

2) Describe control procedures

3) Identify quality control measures

4) Describe standards, practices, and conventions

5) Identify risks

ix) Maintenance records and reports

1) Describe how information will be collected and provided

2) Lists of requests for assistance, modification requests, or problem reports

3) Status of requests by categories

4) Priorities of requests

5) Measurement data to be collected on maintenance activities

3.5 Control System Hardware, Firmware and Software Retirement Plan

i) Introduction

1) Describe the system to be retired

2) Identify the final status of the software

3) Describe why retirement is needed

4) Identify the maintainer/support organization

5) Identify the specific software processes retired

6) Describe any retirement protocols between customer and supplier

7) Identify where retirement will be performed

8) Identify when retirement will commence

9) Identify costs to provide retirement

10) Identify the retirement schedule

ii) Hardware Retirement

1) Identify all components to be retired

2) Identify where the components are located

3) Identify special tools and equipment needed for removal

4) Identify special disposal requirements (CRTs. Batteries, electronic boards, etc)

5) Documents all hardware disposal

iii) Firmware Retirement

1) Identify all components storing firmware

2) Identify licensing requirements specific to the firmware

3) Follow all licensing requirements with respect to disposal

4) Identify where the components are located

5) Identify special tools and equipment needed for removal

6) Identify special disposal requirements (CRTs. Batteries, electronic boards, etc)

7) Documents all firmware disposal

iv) Software Retirement

1) Identify all software to be retired

2) Identify licensing requirements specific to the software

3) Follow all licensing requirements with respect to disposal

4) Identify where the software is located

5) Identify special tools and equipment needed for removal (uninstallers, electronic shredders, disk formatters, etc)

6) Identify special disposal requirements of the software storage media (disks, tapes, memory)

7) Documents all software disposal

v) Develop Consolidated Retirement Report and Archive

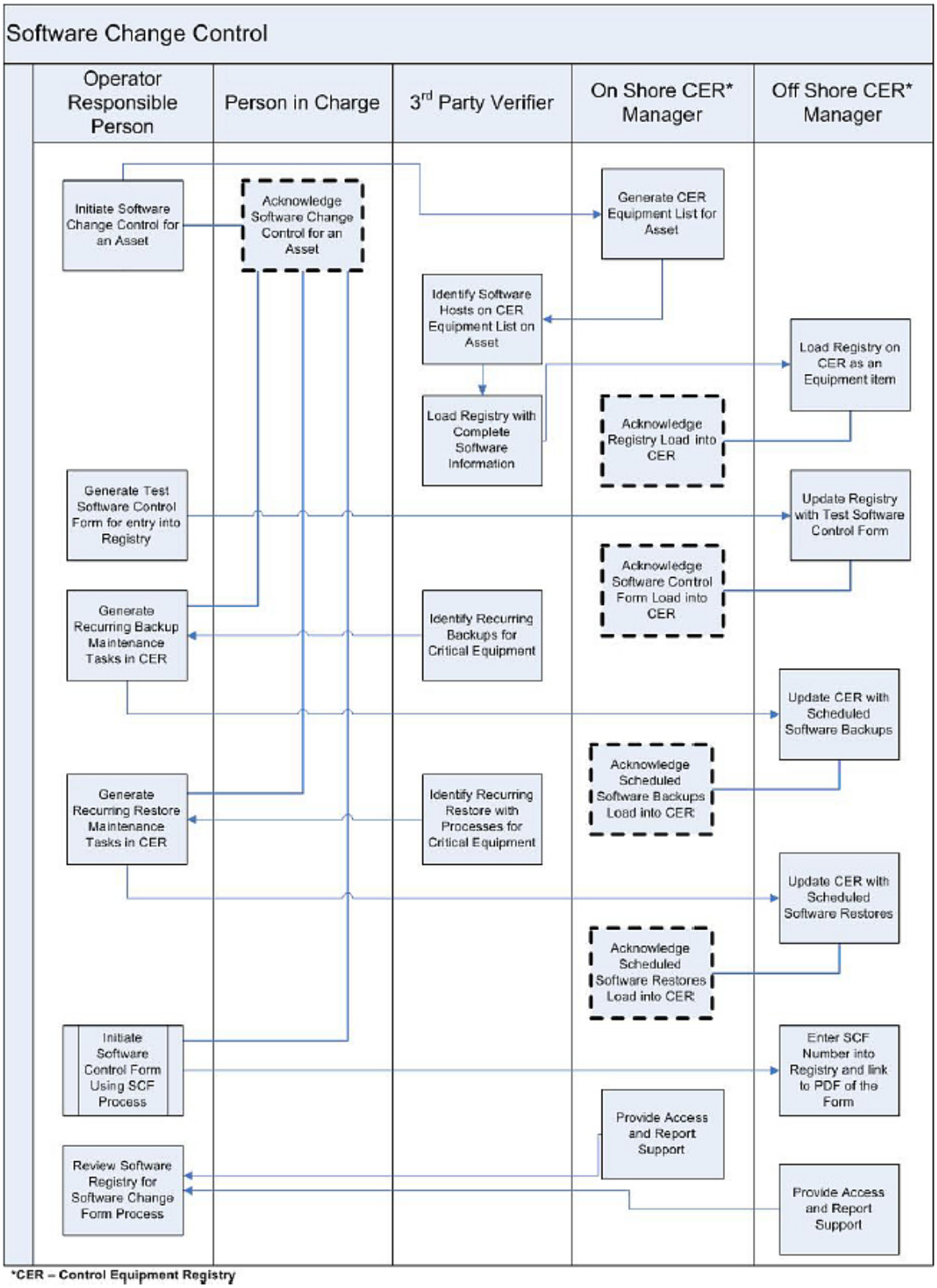
1) Hardware Document

2) Firmware Document

3) Software Document

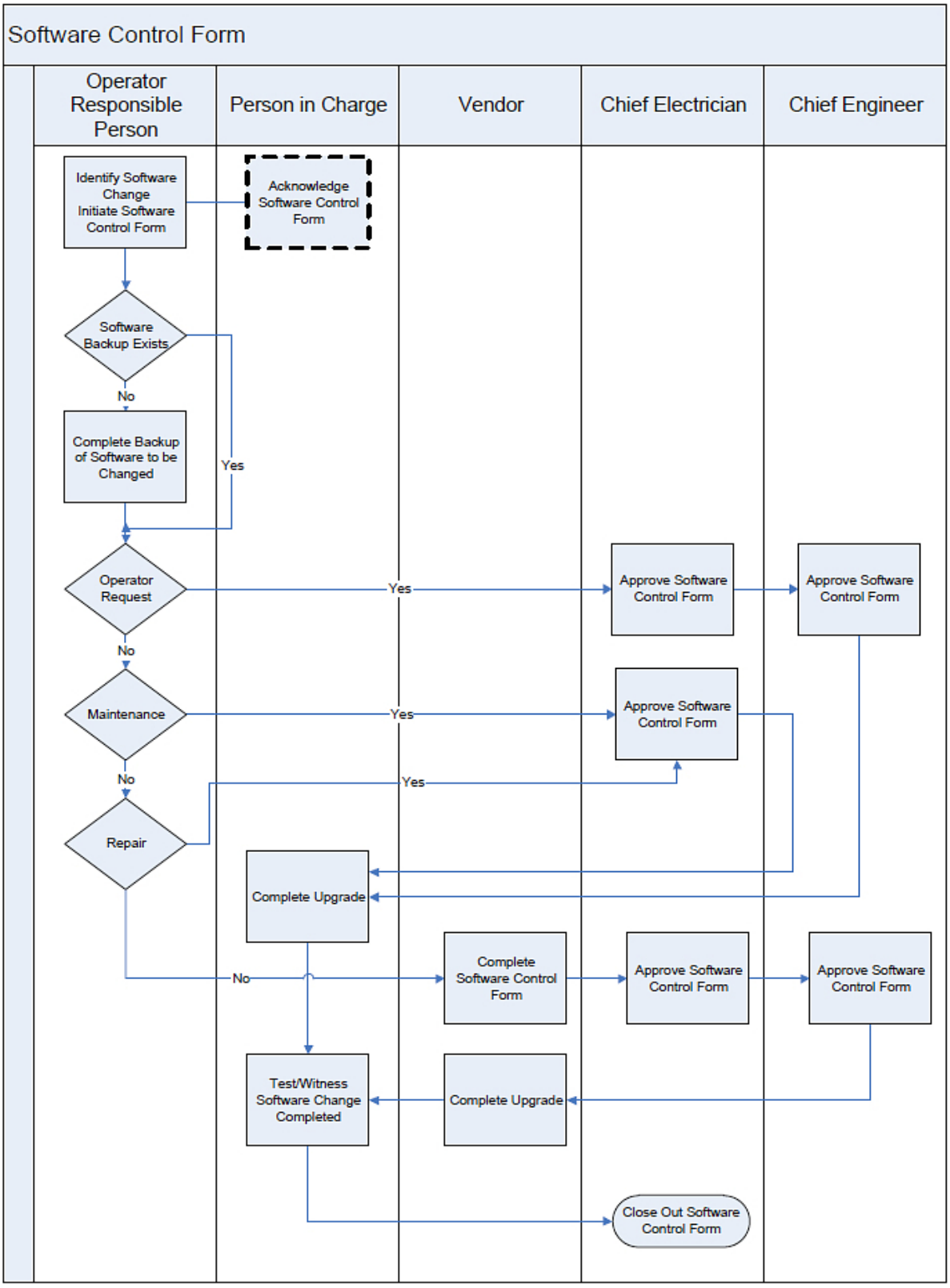
5 Software Change Control Process *(1 September 2012)*

It is recommended that the Owner/DCO reviews the Software Change Control Process to determine completeness. The following figure is an example of a recommended process.


Software Change Control
Operator Responsible Person
Person in Charge
3rd Party Verifier
On Shore CER* Manager
Off Shore CER* Manager
Initiate Software Change Control for an Asset
Acknowledge Software Change Control for an Asset
Generate CER Equipment List for Asset
Identify Software Hosts on CER Equipment List on Asset
Load Registry on CER as an Equipment item
Load Registry with Complete Software Information
Acknowledge Registry Load into CER
Generate Test Software Control Form for entry into Registry
Update Registry with Test Software Control Form
Acknowledge Software Control Form Load into CER
Generate Recurring Backup Maintenance Tasks in CER
Identify Recurring Backups for Critical Equipment
Update CER with Scheduled Software Backups
Acknowledge Scheduled Software Backups Load into CER
Generate Recurring Restore Maintenance Tasks in CER
Identify Recurring Restore with Processes for Critical Equipment
Update CER with Scheduled Software Restores
Acknowledge Scheduled Software Restores Load into CER
Initiate Software Control Form Using SCF Process
Enter SCF Number into Registry and link to PDF of the Form
Provide Access and Report Support
Review Software Registry for Software Change Form Process
Provide Access and Report Support
*CER – Control Equipment Registry

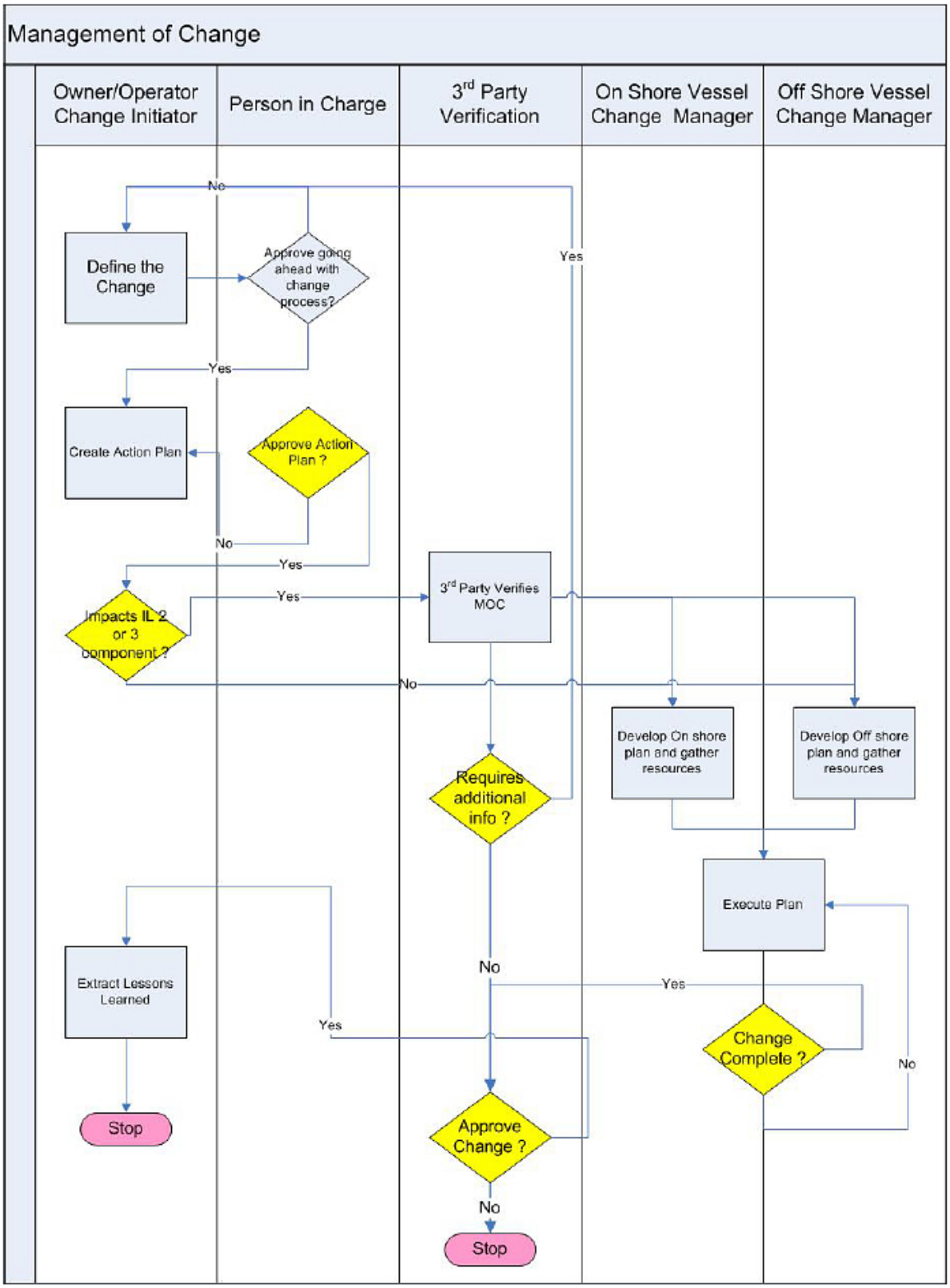
7 Example Software Control Form Process Flow

The following is the process for handling software change control forms.



9 Example MOC Process

FIGURE 1
Recommended Management of Change Process



Recommended inclusions to the retirement or replacement plan

i) Introduction

ii) Describe the system to be Retired

iii) Identify the final status of the software

iv) Describe why retirement is needed

v) Identify the maintainer/support organization

vi) Identify the specific software processes retired

vii) Describe any retirement protocols between customer and supplier

viii) Identify where retirement will be performed

ix) Identify when retirement will commence

x) Identify costs to provide retirement

xi) Identify the retirement schedule

Hardware Retirement

i) Identify all components to be retired

ii) Identify where the components are located

iii) Identify special tools and equipment needed for removal

iv) Identify special disposal requirements (CRTs. Batteries, electronic boards, etc)

v) Document all hardware disposal

Firmware Retirement

i) Identify all components storing firmware

ii) Identify licensing requirements specific to the firmware

iii) Follow all licensing requirements with respect to disposal

iv) Identify where the components are located

v) Identify special tools and equipment needed for removal

vi) Identify special disposal requirements (CRTs. Batteries, electronic boards, etc)

vii) Document all firmware disposal

Software Retirement

i) Identify all software to be retired

ii) Identify licensing requirements specific to the software

iii) Follow all licensing requirements with respect to disposal

iv) Identify where the software is located

v) Identify special tools and equipment needed for removal(uninstallers, electronic shredders, disk formatters, etc)

vi) Identify special disposal requirements of the software storage media (disks, tapes, memory)

vii) Document all software disposal

Develop Consolidated Retirement Report and Archive

i) Hardware Document

ii) Firmware Document

iii) Software Document

11 Obsolete Control System Components Considerations

a) PC Workstations and laptops may be considered obsolete when any of the following milestones occur:

i) The unit is five or more years old.

ii) PC components such as RAM, CPU chipset and processor speed, and hard drive capacity do not meet the minimum requirements of necessary software applications.

iii) The manufacturer's web site no longer offers support for that model.

b) PC Peripherals may be considered obsolete when any of the following milestones occur:

i) The model has been discontinued for three years (unless warranted).

ii) The manufacturer ceases business or is bought by a competitor (unless they support it).

iii) The manufacturer does not provide suitable device drivers for the operating system(s).

c) PC Applications may be considered obsolete when any of the following milestones occur:

i) The software version is three or more generations out of date.

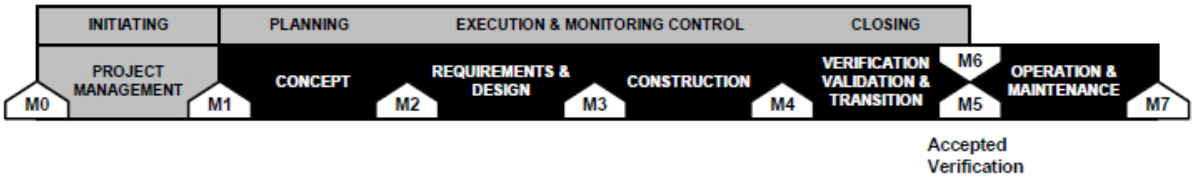
ii) The manufacturer ceases business or is bought by a competitor (unless they support it).

iii) The manufacturer fails to correct any significant security flaw in a timely manner.

iv) The application will not install cleanly or run safely on the current OS.

APPENDIX **8**

Project Management



1 Scope

Project management is the application of knowledge, skills, tools, and techniques that enables the initiation, planning, execution, monitoring and control, and closure of a project within a given schedule and budget, and with the expected level of quality to satisfy project requirements and objectives.

3 Background

The Project Management Institute's Project Management Body of Knowledge (PMBOK®), the application of knowledge, skills, tools, and techniques have been implemented in processes that are depicted in A8/3 TABLE 1. The differentiation between core processes and facilitating (support) processes. Each process group may contain core and support processes. Core processes are those that occur in sequence.

Project management results in the creation of deliverables, and utilizes milestones to mark the plan's progress. In the following discussion, it is noted that the focus is on project management processes where the milestones and deliverables are relatively independent from the Software Development Life Cycle (SDLC), noted in white in A8/5 FIGURE 1, milestones and deliverables.

TABLE 1
39 Project Processes

Knowledge Area					
Process Group	***Integration***	***Scope***	***Time***	***Cost***	***Quality***
Initiating		***Initiation***			
Planning	Project Plan Development	Scope Planning Scope Definition	Activity Definition Activity Sequencing Activity Duration Estimating Schedule development	Resource Planning Cost Estimating Cost Budgeting	Quality Planning
Executing	Project Plan Execution				Quality Assurance
Monitoring and Controlling	Integrated Change Control	Scope Verification Scope Change Control	Schedule control	Cost control	Quality Control
Closing					
Underline = Core Process, non-underline – Facilitating processes					

From IEEE 1490-2003 IEEE Guide Adoption of PMI Standard A Guide to the Project Management Body of Knowledge

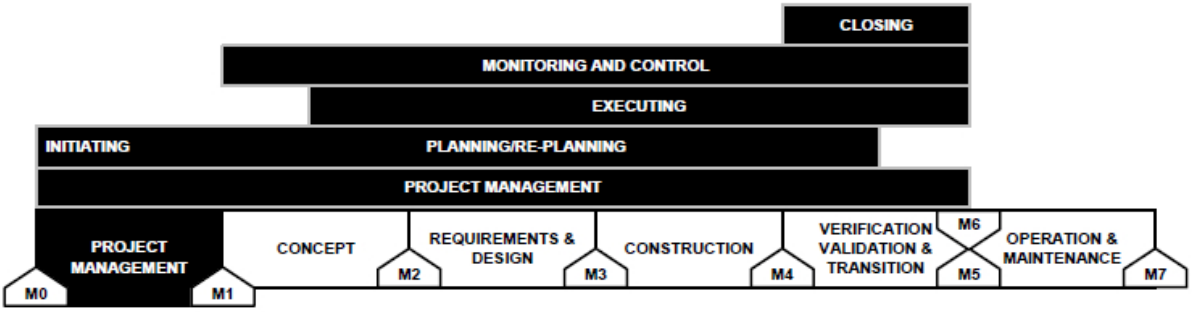
Knowledge Area				
Process Group	***HR***	***Communication***	***Risk***	***Procurement***
Initiating				
Planning	Organization Planning Staff acquisition	Communication Planning	Risk Management Planning Risk Identification Qualitative Risk Analysis Quantitative Risk Analysis Risk Response Planning	Procurement Planning Solicitation Planning
Executing	Team Development	Information Distribution		Solicitation Source selection Contract Administration
Monitoring and Controlling		Performance Reporting	Risk Monitoring and Control	
Closing		Administrative Closure		Contract Closeout
Underline = Core Process, non-underline – Facilitating processes				

From IEEE 1490-2003 IEEE Guide Adoption of PMI Standard A Guide to the Project Management Body of Knowledge

5 PM Process Groups

A8/5 FIGURE 1 below depicts the relationship between the Project Management Process groups and the SDLC.

FIGURE 1
Project Management Process Groups Relationship to SDLC



5.1 PM Initiating Group

5.1.1 Description

Initiating is a process group that contains the fewest number of processes and where the scope of the project is first addressed. Other activities that occur during initiation:

i) Clarifying the concept and objectives of the project

ii) Obtaining commitment from the other Stakeholders

iii) Obtaining positive agreement from stakeholders regarding:

- Scope, key expectations, project environment, contractual terms, budget, financial arrangements, critical success factors, risks, etc.

iv) Transferring responsibility for the project to the project manager so that the project manager understands:

- Human resources, budget, communications, environment specifics (safety, compliance, etc.) outsourcing policies and critical success factors

5.1.2 Initiating Process Group Summary

The initiating group contains these activities:

i) Authorizing the project or phase

ii) Assignment of the Project Manager

iii) Establishment of financial guidelines and accounts (budget)

5.1.3 Initiating Group Deliverables

The Initiating Group deliverables are:

i) Brief summary of the objectives and goals of the project listing key personnel or stakeholders

ii) Initial preliminary SDLC schedule

iii) Initial preliminary overall project schedule

iv) Initial preliminary Work Breakdown Structure (WBS)

v) Estimated software size measured in lines of code (LOC), function points (FP), number of features or some other sizing measure

5.1.4 Initiating Group PM Marker

PM Initiating Group PM Marker is:

Start of the Concept Phase activities. In order to achieve this PM Marker:

i) Project authorized

ii) Resources assigned

iii) Progress report expectations defined

iv) Communication avenues developed and published

5.3 PM Planning Group

5.3.1 Planning Group Description

Planning takes the general to the specific. Early in the SDLC, the WBS may not be able to be populated with great detail as the detail is not available until the SDLC starts.

Planning is a process group that contains the most processes. Planning processes depicted in 3/2.2.3 TABLE 1 cross all knowledge areas and consist of both core and supportive processes. Software development plan is incorporated into the project plan for the overall project.

The dynamic nature of software development may lead to adjustments in the requirements or specifications, hence the need to revise existing plans.

5.3.2 Planning Group Summary

The planning group is a dynamic process group with activities spanning the SDLC.

i) Project plan development

ii) Scope planning and definition

iii) Activity definition and sequencing

iv) Activity duration estimating

v) Schedule development

vi) Resource planning

vii) Quality, organizational and communication planning

viii) Communication

ix) Risk identification

x) Risk response and management planning

xi) Qualitative and quantitative risk analysis

xii) Procurement and Solicitation Planning

xiii) Cost estimate

xiv) Budgeting

xv) Staff acquisition

5.3.3 Planning Group Deliverables

The Planning Group Deliverables are:

i) The detailed software development plan which depicts what resources will be used to complete the elements of the WBS that drives the SDLC. That plan integrates the schedule for the SDLC phase (and overall project at a higher level) and the resource profile. This plan will be useful for the monitoring and control phases.

ii) Software development plan is incorporated into the project plan for the overall project.

5.3.4 Planning Group PM Marker

The establishment of PM markers (or PM stage gates) for the planning process group addresses the needs of the project manager especially in accurate reporting to the Owner:

i) Completion of the project (or SDLC) phase schedule

ii) Completion of the project (or SDLC) financial plan

iii) Completion of resource plan

5.3.5 Planning Group Metrics

It is recommended to collect the following data:

i) *Schedule plans.* Performance to schedule is the resulting measure.

ii) *Financial plan.* Performance to budget is the resulting measure.

iii) *Staffing (resource) plan.* Calculation of effective utilization is the resulting measure.

iv) *Software Size:* Whether the size measure is lines of code (LOC), function points (FP), number of features or some other sizing measure: overall performance metrics require this measure.

v) *Defects:* Depending on the Owner's interest, all defects, or defects with a minimum IL threshold may be counted. The points in the schedule that they are discovered are used to develop defect discovery rates. Defect discovery rates are combined with staffing profiles and other factors, defect density and defects other forecasts can be generated.

5.5 PM Executing Group

5.5.1 Executing Group Description

Executing a project encompasses project processes and activities to get the work done as planned in the approved project plan. The plan calls for the accumulation of actual data compared against that plan. The execution of the project plan overlaps significantly with the monitoring and control process group because it is the execution against the plan that enables the monitoring. For the project manager, this involves meeting with team members, team focus, team development, resolving conflicts and problems, securing the necessary resources to accomplish the project, facilitating quality assurance, and communicating with stakeholders. When vendors are involved, executing a project may also include vendor-related activities such as: solicitation, selection, and contract administration.

5.5.2 Executing Group Summary

The executing process group's widest-ranging activity is project plan execution. Plan execution is performed for the SDLC through the V V&T Phase.

i) Project plan execution

ii) Quality assurance

iii) Team Development

iv) Information Distribution

v) Solicitation (if applicable)

vi) Source selection (if applicable)

vii) Contract administration (if applicable)

5.5.3 Executing Group Deliverables

During the executing process, the typical deliverables are the same ones that are listed in the SDLC from Concept through V V & T Phase.

5.5.4 Executing Group PM Markers

PM Markers generally include those Milestones that are in the SDLC.

5.5.5 Executing Group Metrics

Generally there are no metrics developed for the executing group, however actual expenditure of resources in terms of person hours and schedule days is to be collected. Most metrics are derived using monitoring and controlling processes based on the planning processes.

5.7 PM Monitoring and Control Group

5.7.1 Monitoring and Control Group Description

The monitoring and control group involves tracking the progress of the project comparing the actual data against the plan. Cost, quality and schedule control are possible only if there are processes that allow the comparison of actuals to either plans, internal or industry data. This is an area where third party data can enable benchmarking.

5.7.2 Monitoring and Controlling Group Summary

These activities are performed across the SDLC from Concept through the V V&T Phase.

5.7.3 Monitoring and Controlling Group Deliverables *(1 September 2012)*

Monitoring and Controlling Group deliverables are:

i) It is recommended that Schedule and reports of performance to schedule are submitted by the SI.

ii) Cost target reports and the corrective plan(s) are to be provided to the Owner

iii) Peer review inspections of specification, design, and test planning documents are provided to the IA.

iv) Variance to standards report(s)

v) Software Size measured in lines of code (LOC) function points (FP), number of features or some other sizing measure,

5.7.4 Monitoring and Control Group PM Markers *(1 September 2012)*

PM Markers include:

i) SI internal testing percentage complete

ii) Development deliverables complete

iii) Maintenance manuals and drawings are complete and ready to turn over to the DCO organization

5.7.5 Monitoring and Control Group Metrics

The minimum set of data to be collected includes:

i) Estimated number of Supplier's packages

ii) Software Size measured in lines of code (LOC) function points (FP), number of features or some other sizing measure Duration. Actual milestone completion vs. plan

iii) Peak Staff

iv) Reliability. Actual defects discovered by severity vs. plan

5.9 PM Closing Group

5.9.1 Closing Group Description

Closing processes provides delivered functionality. Complete documentation is delivered to the Owner for use during the Operation and Maintenance Phase.

5.9.2 Closing Group Summary

Closing a project consists of delivering the end product to the customer and overseeing transition functions such as training and others.

5.9.3 Closing Group Deliverables

The Closing Group deliverables are:

i) Deliverable summation reports noting any open issues

ii) Certification of customer receipt of all documentation.

5.9.4 Closing Group PM Markers

Two PM markers are expected during the closing process:

i) End of the V V & T Phase where verification is accepted and validation of the software.

ii) Start of the Operations and Maintenance Phase beginning with transition of documentation, updated with changes made to the software during commissioning, and ongoing maintenance during operation of the unit.

5.9.5 Closing Group Metrics

The data that are to be collected for the closing group includes final size, effort (person-days) and defect count. Start and end dates of all SDLC phases are to be collected as well as the staffing profiles for each phase, by resource or role type if possible.

7 Software Project Management Plan (SPMP)

The basic template to be used is derived from IEEE Std 1058-1998, *IEEE Standard for Software Project Management Plans*. The following is a template for the SPMP. It begins with a cover page that contains the version control and release information. Each section has a description of the information contained within. It is recommended that a Review of Chapter 7 of IEEE Std 1058-1998, *Defining the Goal and Scope of the project*, before filling in the SPMP template.

Software Project Management Plan

for

<Name of Project>

<author>

<date>

Version	Release Date	Responsible Party	Major Changes
0.1			Initial Document Release for Comment

8 Table of Contents

Build the table of contents here. Insert it when you finish your document.

9 Introduction

This section of the SPMP provides an overview of the project.

9.1 Project Overview

Include a concise summary of the project objectives, major work activities, major milestones, required resources, and budget. Describe the relationship of this project to other projects, if appropriate. Provide a reference to the official statement of product requirements.

9.3 Project Deliverables

List the primary deliverables for the customer, the delivery dates, delivery locations, and quantities required satisfying the terms of the project agreement.

9.5 Evolution of the SPMP

Describe how this plan will be completed, disseminated, and put under change control. Describe how both scheduled and unscheduled updates will be handled.

9.7 Reference Materials

Provide a complete list of all documents and other sources of information referenced in the plan. Include for each the title, report number, date, author, and publishing organization.

9.9 Definitions and Acronyms

Define or provide references to the definition of all terms and acronyms required to properly interpret the SPMP.

11 Project Organization

This section specifies the process model for the project and its organizational structure.

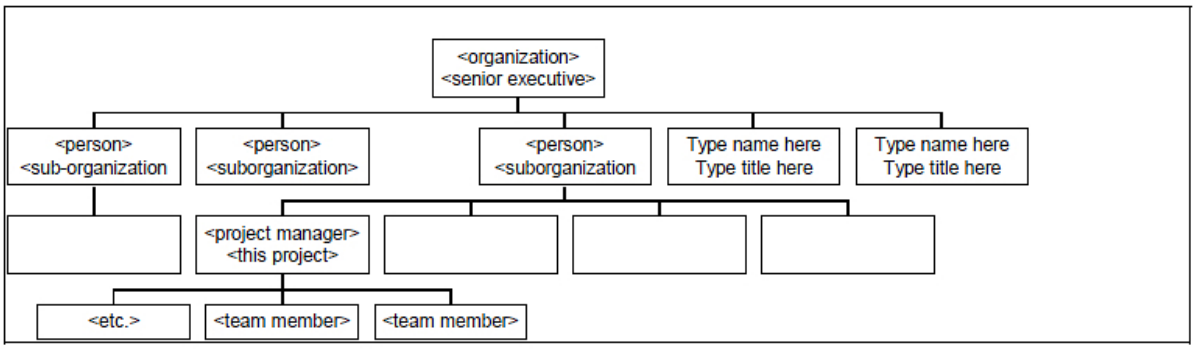
11.1 Process Model

Specify the life cycle model to be used for this project or refer to an organizational standard model that will be followed. The process model includes roles, activities, entry criteria and exit criteria for project initiation, product development, product release, and project termination.

11.3 Organizational Structure

Describe the internal management structure of the project, as well as how the project relates to the rest of the organization. It is recommended that charts be used to show the lines of authority.

Example Organization Chart



11.5 Organizational Interfaces

Describe the administrative and managerial interfaces between the project and the primary entities with which it interacts. A table may be a useful way to represent this.

Organization Interfaces

Organization	Liaison	Contact Information
Customer: <name>	<name>	<phone, email, etc.>
Subcontractor: <name>		
Software Quality Assurance		
Software Configuration Management		
<etc>		

11.7 Project Responsibilities

Identify and state the nature of each major project function and activity, and identify the individuals who are responsible for those functions and activities. Tables of functions and activities may be used to depict project responsibilities.

Project Responsibilities

Role	Description	Person
Project Manager	leads project team; responsible for project deliverables	<name>
Technical Team Leader(s)	<define as locally used>	<name>
<etc.>	<etc.>	

13 Managerial Process

This section of the SPMP specifies the management process for this project.

13.1 Management Objectives and Priorities

Describe the philosophy, goals, and priorities for managing this project. A flexibility matrix might be helpful in communicating what dimensions of the project are fixed, constrained and flexible. Each degree of flexibility column can contain only one "X".

Flexibility Matrix

Project Dimension	Fixed	Constrained	Flexible
Cost		X	
Schedule	X		
Scope (functionality)			X

13.3 Assumptions, Dependencies, and Constraints

State the assumptions on which the project is based, any external events the project is dependent upon, and the constraints under which the project is conducted. Include an explicit statement of the relative priorities among meeting functionality, schedule, and budget for this project.

13.5 Risk Management

Describe the process to be used to identify, analyze, and manage the risk factors associated with the project. Describe mechanisms for tracking the various risk factors and implementing contingency plans. Risk factors that are considered include contractual risks, technological risks, risks due to size and complexity of the product, risks in personnel acquisition and retention, and risks in achieving customer acceptance of the product. The specific risks for this project and the methods for managing them may be documented here or in another document included as an appendix or by reference.

13.7 Monitoring and Controlling Mechanisms

Define the reporting mechanisms, report formats, review and audit mechanisms, and other tools and techniques to be used in monitoring and controlling adherence to the SPMP. Project monitoring occurs at the level of work packages. Include monitoring and controlling mechanisms for the project support functions (quality assurance, configuration management, documentation and training).

A table may be used to show the reporting and communication plan for the project. The communication table can show the regular reports and communication expected of the project, such as weekly status reports, regular reviews, or as-needed communication. The exact types of communication vary between groups, but it is useful to identify the planned means at the start of the project.

Communications and Reporting Plan

Information Communicated	From	To	Time Period
Status report	Project Team	Project Manager	Weekly
Status report	Project Manger	Software Manager, Project Team	Weekly
Project Review	Project Team	Software Manager	Monthly
<etc>			

13.9 Staffing Approach

Describe the types of skills required for the project, how appropriate personnel will be recruited, and any training required for project team members.

15 Technical Process

This section specifies the technical methods, tools, and techniques to be used on the project. It also includes identification of the work products and reviews to be held and the plans for the support group activities in user documentation, training, software quality assurance, and configuration management.

15.1 Methods, Tools, and Techniques

Identify the computing system(s), development method(s), standards, policies, procedures, team structure(s), programming language(s), and other notations, tools, techniques, and methods to be used to specify, design, build, test, integrate, document, deliver, modify or maintain the project deliverables

15.3 Software Documentation

Specify the work products to be built for this project and the types of peer reviews to be held for those products. It may be useful to include a table that is adapted from the organization's standard collection of work products and reviews. Identify any relevant style guide, naming conventions and documentation formats. In either this documentation plan or the project schedule provide a summary of the schedule and resource requirements for the documentation effort.

The following documentation is required as a minimum for requirements implementation:

15.3.1 Software Requirements Specification (SRS)

The SRS clearly and precisely describes each of the essential requirements (functions, performances, design constraints, and attributes) of the software and the external interfaces. Each requirement is defined such that its achievement is capable of being objectively verified and validated by a prescribed method, for example, inspection, analysis, demonstration, or test.

15.3.2 Software Design Description (SDD)

The SDD describes the major components of the software design including databases and internal interfaces.

15.3.3 Software Test Plan

The Software Test Plan describes the methods to be used for testing at all levels of development and integration: requirements as expressed in the SRS, designs as expressed in the SDD, code as expressed in the implemented product. The test plan also describes the test procedures, test cases, and test results that are created during testing activities.

15.5 User Documentation

Describe how the user documentation will be planned and developed. (This may be just a reference to a plan being built by someone else.) Include work planned for online as well as paper documentation, online help, network accessible files and support facilities.

15.7 Project Support Functions

Provide either directly or by reference, plans for the supporting functions for the software project. These functions may include, but are not limited to, configuration management, software quality assurance, and verification and validation. Plans for project support functions are developed to a level of detail consistent with the other sections of the SPMP. In particular, the responsibilities, resource requirements, schedules and budgets for each supporting function are specified.

17 Work Packages, Schedule, and Budget

Specify the work packages, dependency relationships, resource requirements, allocation of budget and resources to work packages, and a project schedule. Much of the content may be in appendices that are living documents, updated as the work proceeds.

17.1 Work Packages

Specify the work packages for the activities and tasks that are completed in order to satisfy the project agreement. Each work package is uniquely identified. A diagram depicting the breakdown of project activities and tasks (a work breakdown structure) may be used to depict hierarchical relationships among work packages.

17.3 Dependencies

Specify the ordering relations among work packages to account for interdependencies among them and dependencies on external events. Techniques such as dependency lists, activity networks, and the critical path method may be used to depict dependencies among work packages.

17.5 Resource Requirements

Provide, as a function of time, estimates of the total resources required to complete the project. Numbers and types of personnel, computer time, support software, computer hardware, office and laboratory facilities, travel, and maintenance requirements for the project resources are typical resources that are specified.

17.7 Budget and Resource Allocation

Specify the allocation of budget and resources to the various project functions, activities, and tasks.

17.9 Schedule

Provide the schedule for the various project functions, activities, and tasks, taking into account the precedence relations and the required milestone dates. Schedules may be expressed in absolute calendar time or in increments relative to a key project milestone.

19 Additional Components

Certain additional components may be required and may be appended as additional sections or subsections to the SPMP. Additional items of importance on any particular project may include subcontractor management plans, security plans, independent verification and validation plans, training plans, hardware procurement plans, facilities plans, installation plans, data conversion plans, system transition plans, or the product maintenance plan.

19.1 Index

An index to the key terms and acronyms used throughout the SPMP is optional, but recommended to improve usability of the SPMP.

19.3 Appendices

Appendices may be included, either directly or by reference, to provide supporting details that could detract from the SPMP if included in the body of the SPMP. Suggested appendices include:

- Current Top 10 Risk Chart
- Current Project Work Breakdown Structure
- Current Detailed Project Schedule

21 Software Quality Assurance Discussion

Below is a discussion following the *Practical Software and Systems Measurement*and the metrics associated with an SQA plan:

21.1 Software Process and Product Metrics

The software process and product metrics enforced by the SQA are defined by the PSM Practical Software and Systems Measurement guide. Only six software process and product metrics are selected from the PSM Practical Software and Systems Measurement Guide, which include software size (process), software effort (process), software cost (process), software productivity (process), software cycle time (process), and software quality (product).

- *Software Size (process):* Physical size and stability measures quantify the physical size of a system or product. Size is a critical factor for estimating development schedules and costs. These measures also provide information on the amount and frequency of change to products, which is especially critical late in product development. The lines of code measure counts the total amount of source code and the amount that has been added, modified, or deleted. Lines of code is a well-understood software measure that helps in estimating project cost, required effort, schedule, and productivity. Changes in the number of lines of code indicate development risk due to product size volatility, and possible additional work.
- *Software Effort (process):* Effort refers to develop effort—the effort required to design, code, unit test, and system test, measured in person-months. The effort measure counts the number of labor hours or number of personnel applied to all tasks. This is a straightforward, easily understood measure. It can be categorized by activity as well as by product. This measure usually correlates directly with cost, but can also address other common issue areas including schedule and progress, and process performance.
- *Software Cost (process):* The cost measure counts budgeted and expended costs. The measure provides information about the amount of money spent on a project or a product, compared to budgets.
- *Software Productivity (process):* Productivity is the number of lines of source code produced per programmer-month (person-month) of effort. The productivity measure compares the amount of product completed to the amount of effort expended. This measure is a basic input to project planning and can evaluate whether performance levels are sufficient to meet cost and schedule estimates. Productivity is also useful early in the project for estimate and baseline comparisons before actual productivity data is available.

- *Software Cycle Time (process):* Cycle time or duration is defined as the elapsed time in hours or months during which development effort proceeds without interruption. Cycle time measures the length of time that it takes a process to complete all associate activities. The accumulation of all processes determines the total schedule to complete a project. Usually, a key objective in process improvement is to reduce overall cycle time.
- *Software Quality (product):* Quality or defect density is the number of software defects committed per thousand lines of software source code. The defects measure quantifies the number, status, and priority of defects reported. It provides useful information on the ability of a supplier to find and fix defects in hardware, software, or documentation. The number of defects indicates the amount of rework, and has a direct impact on quality. Arrival rates can indicate product maturity (a decrease normally occurs as testing is completed). Closure rates are an indication of progress, and can be used to predict test completion. Tracking the length of time that defects have remained open can be used to determine whether progress is being made in fixing defects, or whether rework is being deferred. A defect density measure—an expression of the number of defects in a quantity of product—can be derived from this measure. Defect density can identify components with the highest concentration of defects.

23 Metrics *(1 September 2012)*

Below are the recommended metrics to be collected for each phase, at a minimum.

i) Update the number of Supplier's packages

ii) Software size estimate or actual size in lines of code (LOC), function points (FP), number of features or some other size measure

iii) Actual milestone completion vs. plan

iv) Peak staff estimate

v) Effort expended for this phase

APPENDIX 9

Design Group *(1 September 2012)*

To promote clarity, the following tables show activities of each organization during the execution of all phases. The abbreviations are from the following table:

Phase – Organization – Tracking Number

PHASE		ORGANIZATION	
D =	Design	OW =	Owner (Note 1)
		DCO =	Driller or Crew
		SBI =	Ship Builder Integrator (Shipyard)
CON =	Construction	IA =	Independent Auditor
V V & T =	Verification, Validation & Transition	V & V =	Verification & Validation
OM =	Operate & Maintenance	CT =	Subcontractor

Example: If the Supplier or a Subcontractor in the Design Group has a requirement, deliverable or activity #1, then this activity is "D-CT-R1". If the System Integrator has an activity #5 in the Design Group, then this activity is "D-SI-A5".

The documents and data requested by ABS in Appendix 9 tables are used to support ABS's reviews of the required submittals.

Note:

1 The Owner is the organization which provides funding and initiates the project. The Ship Builder Integrator or Shipyard or Builder may be the Owner during the construction of the vessel or offshore unit.

1 Activities and Submittals for Design Group

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participate in meeting*	*Notes*
D-SBI-R1	Specification	Submit the specification to the ISQM SI for the system. May submit specifications to sub suppliers, per SBI's normal procedure.	ISQM SI		
D-SI-R2	Specification	Submit the specification to the ISQM CT for the system and review specification from shipyard or owner.	ISQM CT	---	Specification becomes part of FDD. No financial or contractual information is to be included in document for FDD. Design Group includes Concept Phase and RD Phase.
D-CT-R3	Specification	Submit the specification to the Non-ISQM CT for the system and review specification from shipyard or owner.	CT	---	Specification becomes part of FDD. No financial or contractual information is to be included in document for FDD. Design Group includes Concept Phase and RD Phase.
D-SI-R4	Copy of ISO9001 certificate	Copy of current ISO9001 certificate	SBI	ABS	If the ISQM SI does not have ISO9001, contact ABS through the SBI.
D-CT-R5	Copy of ISO9001 certificate	Copy of current ISO9001 certificate	SBI	ABS	If the ISQM CT does not have ISO9001, contact ABS through the SBI.
D-SBI-R6	Copy of ISO9001 certificate	Copy of current ISO9001 certificate	ABS	ABS	If the SBI does not have ISO9001, contact ABS.
D-SI-R7	FDD	Functional Description Documents. Also called Functional Design Specification. FDD is to include Operating and Design limits. See ISQM Guide for details, traceability & FMECA quality.	SBI	SBI, OW, DCO, ABS, IA	SBI is to assign IL numbers to functions.
D-CT-R8	FDD	The FDD contains the vendor's FDD as a separate section of the SI's FDD section. The other sections contain suppliers'information to meet the requirements of the *ISQM Guide*.	SBI	SBI, OW, DCO, ABS, IA	Provide to ISQM SI or SBI. Subject to contracts and proprietary information.

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participat e in meeting*	*Notes*
D-SBI-A9	FDD	FDD provided by ISQM SI. SBI to review and comment. SBI manage and pass on FDD to others.	OW, DCO, ABS, IA		Review and comment, should follow the specification. Assign IL numbers to functions. Pass it on to concerned parties.
D-ABS-A10	FDD	Functional Description Documents. Also called Functional Design Specification.	SBI		Review and Comment
D-SI-R11	Recommended verification method(s)	Present verification method(s) used to verify software.	SBI	ABS, IA, OW, DCO	SBI has the option to accept this method or request another.
D-OW-R12	Select verification method	SBI should have input from ISQM SI of the recommended verification method.	ABS, SI, IA, OW, DCO		
D-V & V-R13	Initial V & V Plan	Provide preferred verification method for the system. Mixing of methods is permissible to ABS.	SBI	SBI, OW, DCO, ABS, IA	Owner selects verification method.
D-SI-A14	Safety Review meeting	Safety meeting to review for human factors, may be part of hardware focused FMEA	---	SBI, OW, DCO, ABS, IA, CT as required to complete the review	
D-SI-R15	Safety Review meeting report	If safety meeting was held	SBI	SBI, OW, DCO, ABS, IA, CT as required to complete the review	
D-SI-A16	FMECA	Software focused, top down functional FMECA for IL2 & IL3 systems only	---	SBI, OW, DCO, ABS, IA	Organize and perform the FMECA if the ISQM system is assigned an IL2 or IL3. May use prior FMECA as base and analysis changes, SBI must agree that this option is acceptable.

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participat e in meeting*	*Notes*
D-CT-A17	Attend SI's FMECA, if requested by SI		---	SBI, OW, DCO, ABS, IA	If the SI requests, the CT is to attend the SI's FMECA meeting
D-SI-R18	FMECA Report		SBI	SBI, OW, DCO, ABS, IA	Submit a report on the FMECA performed on the ISQM system that is assigned an IL2 or IL3.
D-ABS-A19	Report Stage Gate M3	Provide report on compliance with ISQM process and any unresolved issues.	SBI		Report Submittal
D-SBI-R20	Grant permission to proceed to the Construction Phase		ABS, IA, SI		The issued FDD for construction has been approved. FDD may be completed during the Construction Phase.
CON-SI-R21	Updated FDD	Updated FDD when 90% of the coding is complete	SBI	SBI, OW, DCO, ABS, IA	Submit an updated FDD with all the changes. Involved parties to review and comment
CON-V & V-R22	V & V Plan	Verification Plan for the ISQM system	SBI	SBI, OW, DCO, ABS, IA, SI	
CON-CT-R23	V & V Plan	Verification Plan if assigned an IL2 or IL3 rating for the provided function	SBI	ABS, IA, SBI, OW, DCO, SI	
CON-SI-A24	Software provided to V & V Organization	Software is provided to V & V Organization for the software verification.	V & V	---	See ISQM V & V tables.
CON-V & V-R25	Simulator Programming Validation	V & V Organization is to state that the simulator programming has been peer reviewed and will test the ISQM software.	SBI	ABS, IA	
CON-SI-R26	Listing of interface registers	Interface tables listing registers, data & commands passed to and from connected control systems	SBI	---	The listing of interface registers to be used by ABS in development of the integration verification. Interface should already be part of the FDD. Follow contractual agreement for submittals.

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participat e in meeting*	*Notes*
CON-CT-R27	Listing of interface registers	Interface tables listing registers, data & commands passed to and from connected control systems	ISQM SI, ABS	---	The listing of interface registers to be used by ABS in development of the integration verification. Interface should already be part of the FDD. Follow contractual agreement for submittals.
CON-SBI-R28	Listing of interface registers	From SI and sub suppliers to and from ISQM systems and other non-ISQM systems	---	---	SBI to use the integration list for integration verification planning. The lists and SBI schedule are the V & V Plan for SBI.
CON-SBI-R29	Integration Verification Plan	May not be needed by SBI for verification witnessing.	Submitt al	ABS, IA	SBI to use the integration list for integration verification planning. The lists and SBI schedule are the V & V Plan for SBI.
CON-ABS-A30	Report Stage Gate M4	Report Submittal			
CON-SBI-A31	Authorization to proceed to V V & T Phase		Submitt al to parties involve d in that system	ABS, IA, SI	
V V & T-SI-R32	Update FDD if required	The FDD contains the vendor's FDD as a separate section of the SI's FDD section. The other sections contain suppliers'information to meet the requirements of the *ISQM Guide*.	SBI	SBI, ABS, IA	The FDD is to be assembled by SBI (shipyard) or the ISQM SI depending upon contractual and proprietary information from the sub-supplier. The sub supplier may not wish to disclose information to the ISQM SI. If this occurs, the FDD is the responsibility of the SBI. A complete FDD is not necessary for the SBI to grant permission to begin coding.

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participate in meeting*	*Notes*
V V & T-CT-R33	Update FDD if required	The FDD contains the vendor's FDD as a separate section of the SI's FDD section. The other sections contain suppliers'information to meet the requirements of the *ISQM Guide*.	SBI	SBI, ABS, IA	The FDD is to be assembled by SBI (shipyard) or the ISQM SI depending upon contractual and proprietary information from the sub-supplier. The sub supplier may not wish to disclose information to the ISQM SI. If this occurs, the FDD is the responsibility of the SBI. A complete FDD is not necessary for the SBI to grant permission to begin coding.
V V & T-SBI-R34	Completed by V V & T Phase	The FDD is specific to a system and the vendor's FDD as a separate section of the SI's FDD section. A DP FDD, PMS FDD, BDCO FDD, etc., is expected. The other sections contain suppliers'information to meet the requirements of the *ISQM Guide*.	ABS, IA, OW	OW, DCO	The FDD is to be assembled by SBI (shipyard) or the ISQM SI depending upon contractual and proprietary information from the sub-supplier. The sub supplier may not wish to disclose information to the ISQM SI. If this occurs, the FDD is the responsibility of the SBI. A complete FDD is not necessary for SBI to grant permission to begin coding. A reviewed and accepted FDD from the SI is necessary for the coding. A DP FDD, PMS FDD, BDCO FDD, etc., is expected.
V V & T-SBI-R35	Completed FDD	Insert Supplier's and Sub-Supplier's FDD into the master FDD provided by SI. SBI to review and submit to ABS, IA, OW, DCO. ABS to manage and pass on FDD.	ABS, IA, OW, DCO	---	Depending on the contractual agreement, this may be done by the ISQM SI or SBI.
V V & T-V & V-R36	Virus Scan Report	Virus scan before and after verification	SBI	ABS, IA	
V V & T-V & V-R37	Execute V & V Plan	ABS is to witness IL2 and IL3 ISQM control system verification.		ABS, IA, (SBI, OW, DCO optional)	

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participat e in meeting*	*Notes*
V V & T-V & V-R38	V & V Defect(s) rankings	Suggested Ranking of defect(s)	SBI	SBI, OW, DCO, ABS, IA	SI has final approval on the defect(s) ranking.
V V & T-SI-A39	Moderate defects with workaround safety review meetings	Safety review meeting(s) and report(s) for moderate defects with workaround(s) where the SBI has agreed to the workaround	SBI	SBI, ABS, OW, DCO, IA	
V V & T-CT-A40	Verification Witnessing	ABS is to witness IL2 and IL3 ISQM control system verification.	---	ABS, IA, (SBI, OW, DCO optional)	
V V & T-CT-R41	V & V Report	Required for all IL1, IL2 and IL3 systems	ABS	SBI, OW, DCO, ABS, IA	Control systems that are connected to ISQM control systems that are assigned IL1, IL2 or IL3 are required to submit a V & V Report.
V V & T-CT-A42	Moderate defects with workaround safety review meetings	Safety meeting for moderate defects where the SBI has agreed to the workaround	SBI	SBI, OW, DCO, IA	Owner approve defect ranking.
V V & T-SI-R43	Results of workaround safety review meeting report	Safety review report of the workaround, as required	SBI	ABS, IA, OW, DCO	
V V & T-CT-R44	Results of workaround safety review meeting report	Safety review report of the workaround, as required	SBI	ABS, IA, OW, DCO	
V V & T-V & V-R45	V & V Report	Verification Report	SBI	SBI, SI, OW, DCO, ABS, IA	
V V & T-ABS-A46	Report Stage Gate M5	Verification of the system has been accepted by Owner.	SBI		Report Submittal
V V & T-SI-R47	O & M Plan Supporting Documentation	Operating, Operator or Operation Manual	SBI	OW, IA, DCO, SBI, ABS, DCO	Part of the Transition portion of the V V & T Phase. This is when the supporting documentation for the O & M Plan is passed to the Owner and DCO.
V V & T-OW-A48	O & M Plan	V V & T Phase, shortly following commissioning	---	---	Part of the Transition portion of the V V & T Phase.

Tracking Number	*Document*	*Description*	*Submit to Whom*	*Reviews or participate in meeting*	*Notes*
V V & T-SBI-A49	Integration Verification Testing	SBI to organize and inform ABS of schedule	---	ABS, IA	
V V & T-SBI-R50	Integration Verification Report	This report could be the listing of registers in either equipment, where data is written to or read from the equipment's register.	All involved parties	ABS, IA, OW, DCO	This could also be a punch list.
V V & T-OW-A51	Report Stage Gate M6	Validation and acceptance of the control system by the Owner	SBI		Acceptance of the control systems